8th International IFAC Symposium on
Dynamics and Control of Process Systems
Preprints Vol.3, June 6-8, 2007, Cancún, Mexico

FAULT-TOLERANT CONTROL OF A REVERSE OSMOSIS DESALINATION PROCESS

Charles W. McFall, Panagiotis D. Christofides, [1]
Yoram Cohen, and James F. Davis

Department of Chemical and Biomolecular Engineering
University of California, Los Angeles, CA 90095

Abstract: Fault-detection and isolation and fault-tolerant control structures are implemented on a reverse osmosis desalination plant. A detailed mathematical model of a simple reverse osmosis plant is first developed. A family of control configurations are identified next, and bounded nonlinear feedback controllers are developed for each configuration. Stability regions of the closed-loop system under each controller are explicitly characterized. A fault-detection and isolation filter is developed for the reverse osmosis system. A supervisory switching law is derived to guarantee closed-loop stability by determining the activation time of fall-back control configurations in the presence of faults in the primary control configuration. The proposed fault-tolerant control scheme is demonstrated in the context of a reverse osmosis system simulation.

Keywords: Hybrid control, Switching logic, Stability regions, Fault-tolerance, Supervisory control, Fault-detection and isolation, multi-input, Reverse Osmosis.

1. INTRODUCTION

System automation and reliability are crucial components of any modern reverse osmosis (RO) plant. The operational priorities are personnel and product water safety, while also meeting environmental and economic demands. Automated RO plants, however, can be vulnerable to faults in several process components that can effect plant operation. Examples of faults can include valve failure, membrane fouling or scaling, sensor data loss, and pump or variable frequency drive failure. Because RO plants run at high pressures, these failures may cause immediate safety risks to plant personnel. These failures can also lead to a decline in the product water quality, rendering it unsafe for public consumption. These safety issues provide strong motivation for the development of fault-detection and isolation (FDI) and fault-tolerant control (FTC) structures that can quickly identify failed actuators and make effective decisions to maintain safe plant operation.

Several contributions have been made in the literature to process control of RO systems. The first paper which proposed an effective closed-loop control strategy for RO utilized multiple SISO control-loops Alatiqi et al. (1989). Step tests were used to perform system identification, resulting in a model that is a linear approximation around the operating point. The control algorithm of MPC was applied to the resulting linear model in Robertson et al. (1996) and Abbas (2006). Experimental system identification and MPC applications can also be found in Assef et al. (1997) and Burden et al. (2001). Liu et al. (2002) and Herold and Neskakis (2001) implemented minimal feedback control on RO desalination systems, powered by renewable energy sources, in the form of digital on/off switching. Some hybrid systems modeling and control work has been published, such as in Gambier and Badreddin (2002). The

[1] Corresponding author (e-mail: pdc@seas.ucla.edu)

goal of this project is to extend the research on RO control systems to include model-based FDIFTC structures.

Fault-tolerant control structures are based on an underlying assumption that there are more control configurations available than required for the given process Siljak (1980) and Yang et al. (1998). The use of the minimum number of control inputs is desirable to minimize unnecessary control action. Fault-tolerant control, in this case, can be achieved through reconfiguration of the control-loops. To implement fault-tolerant control structures on an RO system, first it is necessary to detect and isolate failure events. The results from Mhaskar et al. (2006b) can be directly applied in order to implement FDI on an RO system. Other FTC results relevant to this project can be found in Mhaskar et al. (2006a) and Gani et al. (2006).

This work focuses on FTC of an RO process. First, a detailed mathematical model that adequately describes the process evolution is derived. A family of candidate control configurations are identified, and Lyapunov-based feedback control laws are constructed for each configuration such that closed-loop stability is guaranteed within an associated constrained stability region. Subsequently, an FDI filter that observes the deviation of the process states from the expected closed-loop behavior is developed to detect and isolate actuator failures. A supervisory switching logic is then derived, on the basis of stability regions and FDI filter information, to orchestrate switching between the available control configurations in a way that guarantees closed-loop stability in the event of actuator faults. The effectiveness of the proposed FDIFTC structure is demonstrated through simulation.

2. PROCESS DESCRIPTION AND MODELING

Fig.1 shows a schematic of an elementary RO desalination process. This is a single-unit RO system with no pre-treatment or post-treatment units. Feed brackish or seawater enter the system through the high pressure pump. This high-pressure water then flows across an RO membrane, and low salinity product water permeates. Concentrated brine then continues through a throttling valve and is discharged at atmospheric pressure. The RO plant consists of a high pressure pump, the three automated valves, membrane unit, and required plumbing and tanks. The valve settings can be manipulated in real time based on measurement information which includes the flow velocities.

The first principles model of this system is based on a macroscopic kinetic energy balance. This

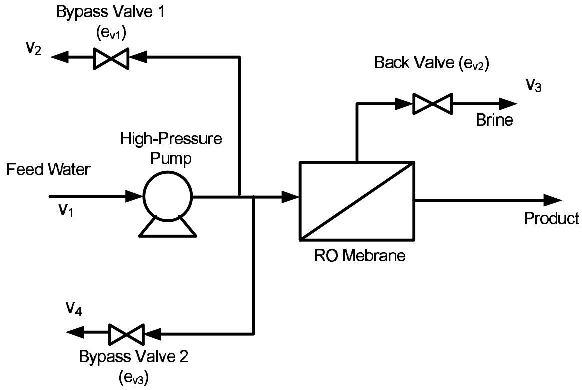

Fig. 1. Single membrane unit reverse osmosis desalination process.

model assumes an incompressible fluid and constant internal volume and mass. Skin friction through piping and the membrane system are negligible relative to hydraulic losses in the throttling valves and across the membrane. Three ordinary differential equations that can describe such a system are derived and they have the following form:

$$\begin{aligned}
\frac{dv_2}{dt} &= \frac{1}{\rho V}\left(\frac{W_p}{v_1(v_2,v_3,v_4)} - \frac{1}{2}e_{v1}v_2\right) \\
\frac{dv_3}{dt} &= \frac{1}{\rho V}\left(\frac{W_p}{v_1(v_2,v_3,v_4)} - \frac{1}{2}e_{v2}v_3\right) \\
\frac{dv_4}{dt} &= \frac{1}{\rho V}\left(\frac{W_p}{v_1(v_2,v_3,v_4)} - \frac{1}{2}e_{v3}v_4\right) \\
v_1 &= -\frac{1}{2}b + \frac{1}{2}\sqrt{b^2+4c} \\
b &= -(v_2+v_3+v_4 - \frac{A_m K_m \Delta\pi}{\rho A_p}) \\
c &= \frac{A_m K_m W_p}{\rho A_p^2}
\end{aligned} \tag{1}$$

where v_1, feed velocity, is a nonlinear function of v_2, v_3, and v_4. v_2, v_3, and v_4 are the velocities of bypass discharge one, brine discharge, and bypass discharge two respectively. ρ is the fluid density, V is the internal volume, W_p is the power delivered by the pump, A_p is the pipe cross sectional area. e_{v1}, e_{v2}, and e_{v3} are the frictional valve constants. A_m is the membrane area, K_m is a membrane mass transfer coefficient, and $\Delta\pi$ is the osmotic pressure. The potential manipulated inputs of the model are the valve constants (e_{v1}, e_{v2}, and e_{v3}) which can be manipulated in practice by an automated electric motor that partially opens or closes the valves. The measured outputs are the velocities of the fluid in the bypass lines, and brine velocity (v_2, v_3, and v_4). Internal pressure, P can be related to feed velocity by $P = \frac{W_p}{v_1 A_p}$. The product velocity, v_5, can be related to the system pressure by $v_5 = \frac{A_m K_m}{\rho A_p}(P - \Delta\pi)$. Table 1 shows the parameter values used for this example.

Table 1. Process parameters and steady–state values

ρ	=	1000	kg/m^3
V	=	10	L
W_p	=	104.4	$Watts$
A_p	=	0.25	in^2
A_m	=	5	m^2
K_m	=	9.218×10^{-9}	s/m
$\Delta\pi$	=	200	psi
e_{v1}^{s1}	=	100	
e_{v2}^{s1}	=	230	
e_{v3}^{s1}	=	10^{-8}	
v_2^{s1}	=	1.0547	m/s
v_3^{s1}	=	0.4625	m/s
v_4^{s1}	=	1.07×10^{-6}	m/s
P^{s1}	=	243.7	psi
e_{v1}^{s2}	=	150	
e_{v2}^{s2}	=	230	
e_{v3}^{s2}	=	300	
v_2^{s2}	=	0.7092	m/s
v_3^{s2}	=	0.4625	m/s
v_4^{s2}	=	0.3546	m/s
P^{s2}	=	243.7	psi

The control objective is to stabilize the process at the desired steady-state. There are at least two unique configurations that will give simultaneous independent control of transmembrane pressure and brine flow-rate. Configuration one, u_1, uses the back valve and the first bypass valve (e_{v1}, e_{v2}) as manipulated inputs. The valves are subjected to input constraints of the form $0 < e_{v1} < 200$ and $130 < e_{v2} < 330$. Configuration two, u_2, uses the back valve with the second bypass valve (e_{v2}, e_{v3}) as manipulated inputs. These valves are subjected to input constraints of the form $130 < e_{v2} < 330$ and $200 < e_{v3} < 400$. The first control configuration, u_1, will be considered as the primary configuration. However, in the event of a failure the plant supervisor may need to implement the fall-back configuration, u_2, to maintain closed-loop stability. By observing the evolution of the plant the FDI filters can detect and isolate an actuator fault. If there is a fall-back control configuration available that is able to stabilize the RO plant, then the supervisor will initiate a mode transition to the fall-back configuration. These issues are addressed in detail in the next section.

3. FAULT-DETECTION AND ISOLATION AND FAULT-TOLERANT CONTROL

Given the properties of the dynamic model, Eq.1, it can be shown that both configurations, u_1 and u_2, satisfy the requirements of achieving fault-detection and isolation of actuator faults (see Mhaskar et al. (2006b) for details). This section discusses the four steps to implement FDIFTC on the RO process. The first step is to synthesize stabilizing feed-back controllers for each configuration. The second step is to explicitly characterize the constrained stability region associated with each configuration. The third step is to design FDI filters for each manipulated input. The final step is to design the switching law that orchestrates the reconfiguration of the control system in a way that guarantees closed-loop stability in the event of faults in the active control configuration.

To present results in a convenient form, the model of Eq.1 is written in deviation variable form around the desired steady state. This is defined as $x = [x_1\ x_2\ x_3]^T$ where $x_1 = v_2 - v_{2_s}$, $x_2 = v_2 - v_{2_s}$, and $x_3 = v_4 - v_{4_s}$. The plant can then be described by the following nonlinear continuous-time system:

$$\begin{aligned} \dot{x}(t) &= f_{k(t)}(x(t)) + g_{k(t)}(x(t))u_{k(t)} \\ |u_{k(t),i}| &\leq u_{k,i}^{max} \\ k(t) \in K &= \{1, 2\} \end{aligned} \tag{2}$$

where $x(t) \in \Re^3$ denotes the vector of process state variables and $u_{k(t)}$ is a vector of inputs where $u_{k,i}(t) \in [-u_{k,i}^{max}, u_k{}^{max}] \subset \Re^3$ denotes the i^{th} constrained manipulated input associated with the k^{th} control configuration. $k(t)$, which takes values in the finite set K, represents a discrete state that indexes the vector fields $f_k(\cdot)$, $g_k(\cdot)$ and the manipulated inputs $u_k(\cdot)$. The explicit form of the vector fields can be obtained by comparing Eqs.1 and 2 and is omitted for brevity. For each value that k assumes in K, the process is controlled via a different set of manipulated inputs which define a given control configuration. Switching between the two available configurations is handled by the high-level supervisor. The control objective is to stabilize the process in the presence of actuator constraints and possible faults. The state feedback problem where measurements of all process states are available for all times is considered to simplify presentation of the results.

3.1 Constrained feedback controller synthesis

In this step we synthesize for each control configuration a feedback controller that enforces asymptotic closed-loop stability in the presence of actuator constraints. To accomplish this task first a quadratic Lyapunov function of the form $V_k = x^T P_k x$ is defined, where P_k is a positive-definite symmetric matrix that satisfies the Riccati inequality. This Lyapunov function is used to synthesize a bounded nonlinear feedback control law for each control-loop (see Lin and Sontag (1991) and El-Farra and Christofides (2003)) of the form:

$$u_k = -r(x, u_k^{max}) L_{\bar{g}_k} V_k \tag{3}$$

where

$$r = \frac{L_{\bar{f}_k}^* V_k + \sqrt{(L_{\bar{f}_k}^* V_k)^2 + (u_k^{max}|L_{\bar{g}_k} V_k|)^4}}{(|L_{\bar{g}_k} V_k|)^2 (1 + \sqrt{1 + (u_k^{max}|L_{\bar{g}_k} V_k|)^2})} \quad (4)$$

and $L_{\bar{f}_k}^* V_k = L_{\bar{f}_k} V_k + \alpha V_k$, $\alpha > 0$. The scalar function $r(\cdot)$ in Eqs.3 and 4 can be considered as a nonlinear controller gain. It can be shown that each control configuration asymptotically stabilizes the states in each mode. This controller gain, which depends on both the size of actuator constraints, u_k^{max}, and the particular configuration used is shaped in a way that guarantees constraint satisfaction and asymptotic stability within a well-characterized region in the state space. The characterization of this region is discussed in the next step.

3.2 Characterization of stability regions

Actuator constraints place fundamental limitations on the initial conditions from which the closed-loop system is asymptotically stable. It is important for the control system designer to explicitly characterize these limitations by identifying, for each control configuration, the set of initial conditions for which the constrained closed-loop system is asymptotically stable. This is necessary for the design of an appropriate switching policy that ensures the fault-tolerance of the closed-loop system. The feedback controller of Eq.3 that is synthesized for each configuration provides such a characterization. Specifically, using a Lyapunov argument, one can show that the set

$$\Theta(u_k^{max}) = \{x \in \Re^3 : L_{\bar{f}_k}^* V_k \leq u_k^{max} |L_{\bar{g}_k} V_k|\} \quad (5)$$

describes a region in the state-space where the control action satisfies the constraints and the time-derivative of the corresponding Lyapunov function is negative-definite along the trajectories of the closed-loop system (see Christofides and El-Farra (2004)). Note that the size of the set depends on the magnitude of the constraints. The set becomes smaller as the constraints become tighter (smaller $u_{k,i}^{max}$). For a given control configuration, the above inequality can be used to estimate the associated stability region. This can be done by constructing the largest invariant subset of Θ, which is denoted by $\Omega(u_k^{max})$. Initial conditions within the set $\Omega(u_k^{max})$ ensure that the closed-loop trajectory stays within the region defined by $\Theta(u_k^{max})$, and thereby V_k continues to decay monotonically, for all times that the kth control configuration is active (see El-Farra and Christofides (2001) for further discussion on this issue). An estimate of $\Omega(u_k^{max})$ is obtained by defining a composite Lyapunov function of the form $V_{C_k} = x^T P_C x$, where P_C is a positive definite matrix, and choosing a level set of V_{C_k}, Ω_{C_k}, for which $\dot{V}_{C_k} < 0$ for all x in Ω_{C_k}. The value c_k^{max} represents a level set on V_{C_k} where $\dot{V}_{C_k} < 0$.

3.3 Fault-detection and isolation filter design

The third step in implementing FDIFTC is that of designing appropriate fault-detection filters. The filters should detect and isolate the occurrence of a fault in an actuator by observing the behavior of the closed-loop process. The FDI filter design for the primary control configuration takes the form:

$$\begin{aligned}
\frac{d\tilde{v}_2}{dt} &= \frac{1}{\rho V}\left(\frac{W_p}{v_1(\tilde{v}_2, v_3, v_4)} - \frac{1}{2} e_{v1}(\tilde{v}_2, v_3, v_4)\tilde{v}_2\right) \\
\frac{d\tilde{v}_3}{dt} &= \frac{1}{\rho V}\left(\frac{W_p}{v_1(v_2, \tilde{v}_3, v_4)} - \frac{1}{2} e_{v2}(v_2, \tilde{v}_3, v_4)\tilde{v}_3\right) \\
r_{1,1} &= |v_2 - \tilde{v}_2| \\
r_{1,2} &= |v_3 - \tilde{v}_3|
\end{aligned} \quad (6)$$

Where $\tilde{v}_2$ and $\tilde{v}_3$ are the filter states for valve one and two respectively. $r_{k,i}$ is the residual associated with the i^{th} input of the k^{th} configuration. The filter states are initialized at the same value as the process states ($\tilde{x}(0) = x(0)$) and essentially predict the evolution of the process in the absence of actuator faults (This assumption can be relaxed, see Mhaskar et al. (2006b)). The residual associated with each manipulated input captures the difference between the predicted evolution of the states in the absence of a fault on that actuator and the evolution of the measured process state. If a given residual becomes non-zero, a fault is declared on the associated input. For a detailed analysis of the FDI properties of the filter, see Mhaskar et al. (2006b).

3.4 Fault-tolerant supervisory switching logic

The final step is to design a switching logic that the plant supervisor will use to decide what fall-back control configuration to implement given an actuator failure. The supervisor should only implement those configurations that will guarantee closed-loop stability and do not utilize a failed actuator. This requires that the supervisor only activates fall-back control configurations for which the state is within the associated stability region at the time of fault-detection. Let the initial actuator configuration be $k(0) = 1$, T_{fault} be the time of an actuator failure, and T_{detect} be the earliest time at which the value of $r_{1,i}(t) > \delta_{r_{1,i}} > 0$ (for the i^{th} input where $\delta_{r_{1,i}}$ is the i^{th} detection threshold). The switching rule given by

$$k(t \geq T_{detect}) = 2 \;\; if \;\; x(T_{detect}) \in \Omega_{C_2}(u_2^{max}) \quad (7)$$

guarantees asymptotic closed-loop stability if u_2 does not include any faulty actuators. The switching law requires monitoring of FDI filters and process state location with respect to fall-back stability regions.

4. SIMULATION RESULTS

A simulation has been performed to demonstrate the implementation of the proposed FDIFTC strategy on the RO plant of Fig.1. The states in the mathematical model given in Eq.1 may not be the system parameters of interest for the operator because bypass flows (v_2 and v_4) do not interact with the membrane unit. Pressure and brine flow, P and v_3, are useful parameters to regulate because they directly effect the membrane unit. Hence, two steady-states have been considered, each one of them has the same system pressure and brine flow rate (v_3), but different bypass flows (v_2 and v_4). The first steady-state corresponds to bypass valve two being closed. The parameters and steady-state values can be seen in Table 1. Under these operating conditions the open-loop system behaves in a stable fashion at each steady-state.

First, nonlinear feedback control under the primary configuration, u_1, was considered. The bounded nonlinear controller was synthesized using Eqs.3 and 4, with $\alpha = 0.1$. The stability region for the primary configuration was estimated using the Lyapunov function, $V_1 = x^T P_1 x$, yielding a $c_1^{max} = 1$ (note: this value of c_1^{max} represents a sufficiently large region of the state space for this simulation, in general much higher values can be considered). Fig.2 shows the evolution of the closed-loop state profiles starting from the initial condition $v_2 = v_3 = 0.1\frac{m}{s}$ and $v_4 = 0.001\frac{m}{s}$ for which $V_1(x(0)) = 0.0263$. Evolution of the system pressure is shown in Fig.3. Since the initial state was within the stability region of the primary control configuration, $V_1(x(0)) = 0.0263 \leq c_1^{max} = 1$, the primary control configuration was able to stabilize the system at the desired steady-state.

Next, a fault in the primary configuration (in e_{v1} specifically) at a time $T_{fault} = 10\ s$ was considered. In this case the fall-back configuration, u_2, was available with valve three, e_{v3}, as one of the manipulated inputs. The quadratic Lyapunov function $V_2 = x^T P_2 x$ and $\alpha = 0.1$ was used to design the controller. The stability region was also estimated using V_2 yielding a $c_2^{max} = 1$.

To demonstrate the advantage of operating under the FDIFTC structure consider the case where no control system reconfiguration takes place after T_{fault}. The system is initialized at $v_2 = v_3 = 0.1\frac{m}{s}$ and $v_4 = 0.001\frac{m}{s}$, and the primary control configuration operates normally until the time $T_{fault} = 10\ s$. At this time valve one stops operating and is partially closed, $e_{v1} = 150$. As shown by the solid lines in Figs.2 and 3 the states move away from the desired values, and settle at a new, undesired, steady-state.

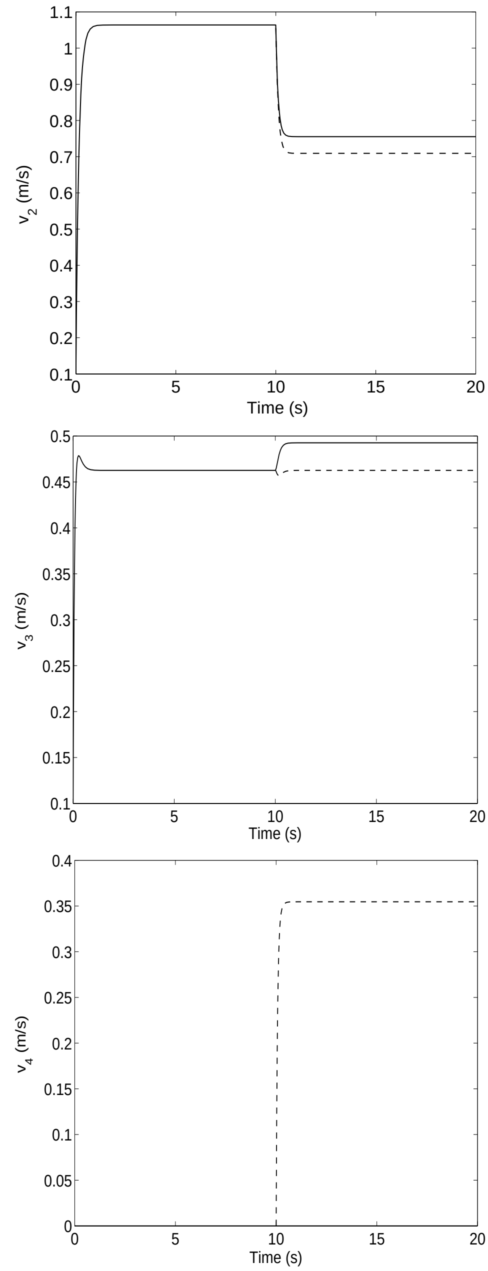

Fig. 2. Evolution of the closed-loop state profiles under fault-tolerant control (dashed line) and without fault tolerant-control (solid line). FTC recovers the desired brine flow, v_3.

However, by implementing the FDIFTC structure the fault can be mitigated. The residual value associated with valve one, $r_{1,1}$, becomes non-zero and reaches the detection threshold, $\delta_{r_{1,1}} = 0.01$, at $T_{detect} = 10.004\ s$ when the fault is declared. The residual value associated with valve two, $r_{1,2}$ remains at zero, indicating that the fault is effecting only valve one. At time T_{detect} the value of the fall-back Lyapunov function is checked against the fall-back stability region to see if switching would guarantee stability. The value of $V_2(x(T_{detect})) = 0.0119 < c_2^{max} = 1$, so reconfiguration to the fall-back controller, $k = 2$, does guarantee closed-loop stability. The evolution of the system states and

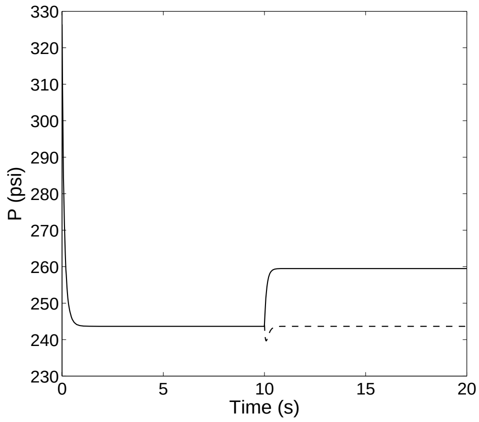

Fig. 3. Evolution of the closed-loop pressure profile under fault tolerant control (dashed line) and without fault tolerant control (solid line). FTC recovers the desired operating pressure.

pressure under the proposed FDIFTC structure can be seen in Figs.2 and 3 (solid lines). This automated reconfiguration allowed the closed-loop system to maintain pressure and brine flow at the desired values.

5. CONCLUSIONS

The focus of this work was to apply recently-developed FDIFTC structures to an RO desalination process model. First, a mathematical model that describes the process evolution was developed. A family of candidate control configurations was then identified, and Lyapunov-based feedback control laws were constructed for each configuration such that closed-loop stability was guaranteed within an associated constrained stability region. An FDI filter that observes the deviation of the process states from the expected closed-loop behavior was developed to detect and isolate actuator failures. A supervisory switching logic was then derived, on the basis of stability regions and FDI filter information, to orchestrate switching between the available control configurations in a way that guarantees closed-loop stability in the event of actuator faults. These ideas were then demonstrated in the context of an RO system simulation. The proposed FDIFTC methodology was able to maintain closed-loop operation at the desired steady-state in the presence of actuator failures.

REFERENCES

A. Abbas. Model predictive control of a reverse osmosis desalination unit. *Desalination*, 194: 268–280, 2006.

I. M. Alatiqi, A. H. Ghabris, and S. Ebrahim. System identification and control of reverse osmosis desalination. *Desalination*, 75:119–140, 1989.

J. Z. Assef, J. C. Watters, P. B. Deshpande, and I. M. Alatiqi. Advanced control of a reverse osmosis desalination unit. *J. Proc. Contr.*, 7: 283–289, 1997.

A. C. Burden, P. B. Deshpande, and J. C. Watters. Advanced control of a b-9 permasep permeator desalination pilot plant. *Desalination*, 133:271–283, 2001.

P.D. Christofides and N.H. El-Farra. *Control of nonlinear and hybrid process systems: designs for uncertainty, constraints and time delays.* Springer, 2004.

N. H. El-Farra and P. D. Christofides. Integrating robustness, optimality, and constraints in control of nonlinear processes. *Chem. Eng. Sci.*, 56:1841–1868, 2001.

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

A. Gambier and E. Badreddin. Application of hybrid modeling and control technieques to desalination plants. *Desalination*, 152:175–184, 2002.

A. Gani, P. Mhaskar, and P. D. Christofides. Fault-tolerant control of a polyethylene reactor. *J. Proc. Contr. in press*, 16, 2006.

D. Herold and A. Neskakis. A small PV-driven reverse osmosis desalination plant on the island of Gran Canaria. *Desalination*, 137:285–292, 2001.

Y. Lin and E. D. Sontag. A universal formula for stabilization with bounded controls. *Sys. & Contr. Lett.*, 16:393–397, 1991.

C. K. Liu, Jae-Woo Park, R. Migita, and G. Qin. Experiments of a prototype wind-driven reverse osmosis desalination system with feedback control. *Desalination*, 150:277–287, 2002.

P. Mhaskar, A. Gani, N. H. El-Farra, C. McFall, P. D. Christofides, and J. F. Davis. Integrated fault-detection and fault-tolerant control of process systems. *AIChE J.*, 52:2129–2148, 2006a.

P. Mhaskar, C. McFall, A. Gani, P.D. Christofides, and J. F. Davis. Fault-tolerant control of nonlinear systems: Fault-detection and isolation and controller reconfiguration. In *Proceedings of American Control Conference*, pages 5115–5122, Minneapolis, MN, 2006b.

M. W. Robertson, J. C. Watters, P. B. Desphande, J. Z. Assef, and I.M. Alatiqi. Model based control for reverse osmosis desalination processes. *Desalination*, 104:59–68, 1996.

D. D. Siljak. Reliable control using multiple control systems. *Int. J. Contr.*, 31:302–339, 1980.

G. H. Yang, S. Y. Zhang, J. Lam, and J. Wang. Reliable control using redundant controllers. *IEEE Trans. Autom. Contr.*, 43:1588–1593, 1998.