# Chapter 15
# Fault-Tolerant Model Predictive Control of Water Transport Networks

**Abstract** This chapter proposes a reliable fault-tolerant model predictive control applied to drinking water transport networks. After a fault has occurred, the predictive controller should be redesigned to cope with the fault effect. Before starting to apply the fault-tolerant control strategy, it should be evaluated whether the predictive controller will be able to continue operating after the fault appearance. This is done by means of a structural analysis to determine loss of controllability after the fault complemented with feasibility analysis of the optimization problem related to the predictive controller design, so as to consider the fault effect in actuator constraints. Moreover, by evaluating the admissibility of the different actuator-fault configurations, critical actuators regarding fault tolerance can be identified considering structural, feasibility, performance and reliability analyses. On the other hand, the proposed approach allows a degradation analysis of the system to be performed. As a result of these analyses, the predictive controller design can be modified by adapting constraints such that the best achievable performance with some pre-established level of reliability will be achieved. The proposed approach is tested on the Barcelona WTN.

## 15.1 Introduction

WTNs require sophisticated supervisory control strategies to ensure and maintain optimal performance even in faulty conditions. In order to take advantage of these expensive infrastructures, a highly sophisticated real-time control (RTC) scheme is necessary to ensure optimal performance [3, 13]. The RTC scheme in a WTN might be local or global. When control is local, regulation devices only use measurements taken at specific locations. While this control structure is applicable in many simple cases, it may not be the most efficient option for large systems with a highly interconnected and complex sensor and actuator infrastructure. A global control strategy, in contrast, which computes control actions taking into account real-time measurements all through the network, is likely the best way to use infrastructure capacity and all available sensor information. Global RTC deals with the problem of generating control strategies (ahead of time), based on a predictive dynamic model and telemetry readings of the network to optimize operation [13]. The multi-variable and large-scale nature of WTNs have led to the use of some variants of MPC as a global control strategy [15], as discussed in previous chapters.

Global RTC of WTNs needs to be operative even in faulty conditions. This problem calls for the use of fault-tolerant control (FTC) mechanisms after a fault is diagnosed so as to avoid the global RTC stopping every time a fault appears. FTC was developed in order to address the growing demand for plant availability [1]. The aim of FTC is to keep a plant fully operative by designing its control system such that system performance can be kept close to desirable levels and stability conditions can be maintained, not only when the system is in nominal conditions but also in the presence of system component faults; FTC should, at the very least, ensure acceptable degraded performance [11]. Tolerance against faults can be embedded in MPC relatively easily in several different ways, as discussed in [9]:

- Changing the constraints in order to represent the fault effect, with the algorithms for actuator faults being especially easy to adapt.
- Modifying the internal plant model used by the MPC in order to reflect fault influence on the plant.
- Relaxing the nominal control objectives in order to reflect system limitations under faulty conditions.

Reviewing the literature, the inclusion of fault tolerance in MPC has already been considered by several authors, including [30], who provides a detailed review of the state-of-the-art in FTC. [4] provides a general overview on how fault tolerance can be embedded in MPC. The inclusion of fault-tolerance in MPC has mainly been addressed by considering practical strategies according to the application domain. For example, [16] described a method for including fault tolerance in MPC for smart grids in order to ensure the proper amount of energy in storage devices and reliable coverage of essential consumer demand. [12] applied fault tolerance in MPC to sewage networks considering a hybrid systems framework. [28] designed a group of predictive controllers to compensate for the fault effects for each component in a wind turbine. More theoretical aspects have also begun to be studied, such as coupling with active fault diagnosis [17] and the use of set-invariance theory [29]. More recent additional objectives for MPC controllers, proposed in [21] and [20], have been to preserve system health and reliability, respectively.

The research presented in this chapter is based on three concepts:

- How fault accommodation/reconfiguration strategies were applied in a linear quadratic regulator (LQR) [23].
- The idea that fault configurations should be evaluated before applying FTC strategies [24].
- The idea of using reliability with the FTC design [7].

Starting from these key ideas, it is proposed a new reliable fault-tolerant MPC scheme for application to WTNs. After a fault has occurred, the MPC controller should be redesigned to cope with the fault by considering either a reconfiguration or an accommodation strategy, depending on knowledge available on the fault. Before starting to apply the FTC strategy, whether the MPC controller will be able to continue operating after the fault appears should be evaluated. This is done in two ways: first, a structural analysis is done to determine the level of loss in post-fault controllability; second, a feasibility analysis is done of the optimization problem related to the MPC design so as to consider the fault effect on actuator constraints. By evaluating the admissibility of different actuator-fault configurations (AFCs), critical actuators regarding fault tolerance can be identified considering structural, feasibility, performance and reliability analyses. This has been studied in [19], where only some of the analyses proposed here were considered.

The approach proposed into this chapter allows a degradation analysis of the system to be performed in terms of performance and reliability. As a result of this analysis, the MPC controller design can be modified, adapting the constraints so as to achieve the best achievable performance with some pre-established level of reliability. The proposed approach was tested in the Barcelona WTN, in an application that also shows that relevant information about critical actuators can be extracted by considering the different analyses proposed.

The main contribution of this chapter is the design of methodologies for the analysis of the influence of faults taking into account reliability features. As discussed, some of the proposed methodologies have been previously documented but not their application in the considered fault tolerance framework, to the best of the knowledge of the authors, after a thorough literature review (a secondary contribution of the chapter).

## 15.2 Problem statement

### *15.2.1 Flow-based control-oriented model*

This chapter considers a general WTN as represented by a digraph $G(\mathcal{V},\mathcal{E})$ (see [22] for more details), where a set of elements, i.e., $n_s$ sources, $n_x$ storage elements, $n_q$ intersection nodes, and $n_d$ sinks, are represented by $v \in \mathcal{V}$ vertices connected by $a \in \mathcal{E}$ links. Due to the network function, water is transported along the links by $n_u$ flow actuators (i.e., pipes and valves), passing through reservoirs or tanks, from specific origin locations to specific destination locations. The network is subject to several capacity and operational constraints, and to measured stochastic flows to customer sinks as driven by water demand.

Selecting the volume in storage elements as the state variable $\mathbf{x} \in \mathbb{R}^{n_x}$, the flow through the actuators as the manipulated inputs $\mathbf{u} \in \mathbb{R}^{n_u}$, and the demanded flow as *additive* measured disturbances $\mathbf{d} \in \mathbb{R}^{n_d}$, the control-oriented model of the WTN may be described by the following set of linear (or linearized) discrete-time difference-algebraic equations (DAE) for all time instants $k \in \mathbb{Z}_+$:

$$\mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k)+\mathbf{B}\mathbf{u}(k)+\mathbf{B}_d\mathbf{d}(k), \tag{15.1a}$$

$$0 = \mathbf{E}_u\mathbf{u}(k)+\mathbf{E}_d\mathbf{d}(k), \tag{15.1b}$$

where the difference equation in (15.1a) describes the dynamics of the storage tanks, and the algebraic equation in (15.1b) describes static relations in the network (i.e., mass balance at junction nodes). Moreover, **A**, **B**, $\mathbf{B}_d$, $\mathbf{E}_u$ and $\mathbf{E}_d$ are time-invariant matrices of suitable dimensions as dictated by the network topology.
System (15.1) is subject to hard state and input polytopic constraints given by:

$$\mathcal{U} \triangleq \left\{\mathbf{u} \in \mathbb{R}^{n_u} \,|\, \mathbf{u}^{\min} \leq \mathbf{u} \leq \mathbf{u}^{\max}\right\}, \tag{15.2a}$$

$$\mathcal{X} \triangleq \left\{\mathbf{x} \in \mathbb{R}^{n_x} \,|\, \mathbf{x}^{\min} \leq \mathbf{x} \leq \mathbf{x}^{\max}\right\}, \tag{15.2b}$$

where $\mathbf{u}^{\min}$, $\mathbf{u}^{\max}$, $\mathbf{x}^{\min}$ and $\mathbf{x}^{\max}$ are the actuator and tank operational limits.

### 15.2.2 Statement of the control problem

The WTN (15.1) is controlled using an MPC law that aims to minimize the operational costs of the WTN as proposed in economic model predictive control (EMPC) [5, 8, 18]. According to [1], the solution of a control problem consists of finding a control law from a given set of *control laws* $\mathbb{U}$, such that the controlled system achieves the *control objectives* $\mathbb{O}$ while its behaviour satisfies a set of *constraints* $\mathbb{C}$. Thus, the solution to the problem is completely defined by the triplet $\langle\mathbb{O},\mathbb{C},\mathbb{U}\rangle$. In the case of an MPC, the triplet $\langle\mathbb{O},\mathbb{C},\mathbb{U}\rangle$ is defined by

$$\mathbb{O}: \qquad \min_{\tilde{\mathbf{x}},\tilde{\mathbf{u}}} J(\tilde{\mathbf{x}},\tilde{\mathbf{u}}), \tag{15.3a}$$

subject to:

$$\mathbb{C}: \tag{15.3b}$$

$$\mathbf{x}(k+i+1|k) = \mathbf{A}\mathbf{x}(k+i|k)+\mathbf{B}\mathbf{u}(k+i|k)+\mathbf{B}_d\mathbf{d}(k+i|k), \qquad \forall i \in \mathbb{Z}_{[0,H_p-1]} \tag{15.3c}$$

$$\mathbf{0} = \mathbf{E}_u\mathbf{u}(k+i|k)+\mathbf{E}_d\mathbf{d}(k+i|k), \quad \forall i \in \mathbb{Z}_{[0,H_p-1]}, \tag{15.3d}$$

$$\mathbf{u}(k+i|k) \in \mathcal{U}, \quad \forall i \in \mathbb{Z}_{[0,H_p-1]}, \tag{15.3e}$$

$$\mathbf{x}(k+i|k) \in \mathcal{X}, \quad \forall i \in \mathbb{Z}_{[1,H_p]}, \tag{15.3f}$$

where

$$\tilde{\mathbf{x}} = \left(\mathbf{x}(1|k),\ldots,\mathbf{x}(N|k)\right), \tag{15.4a}$$

$$\tilde{\mathbf{u}} = \left(\mathbf{u}(0|k),\mathbf{u}(1|k),\ldots,\mathbf{u}(N-1|k)\right), \tag{15.4b}$$

$$\tilde{\mathbf{d}} = \big(\mathbf{d}(0|k), \mathbf{d}(1|k), \ldots, \mathbf{d}(N-1|k)\big) \tag{15.4c}$$

are the state, input and disturbance sequences over $H_p$, respectively. $H_p$ denotes the prediction horizon used by the MPC controller. The sequence $\tilde{\mathbf{d}}$ comes from a forecasting module based on existing time-series techniques (see [15] and [26] for more details).

The MPC law belongs to the set $\mathcal{U}$ and is obtained using the *receding horizon philosophy* [9, 18]. This technique consists of solving the optimization problem (15.3a) from the current time instant $k$ to $k+N$ using $\mathbf{x}(0|k)$ as the initial condition obtained from measurements (or state estimation) at time $k$. Only the first value $\mathbf{u}^*(0|k)$ from the optimal input sequence $\tilde{\mathbf{u}}^*$ (which arises from the solution of the optimization problem (15.3a)) is applied to the system. At time $k+1$, in order to compute $\mathbf{u}^*(0|k+1)$ the optimization problem (15.3a) is solved again from $k+1$ to $k+1+N$ (i.e., the time window is shifted), updating initial states $\mathbf{x}(0|k+1)$ from measurements (or state estimation) at time $k+1$. The same procedure is repeated for the following time instants.

The objective function $J$ in (15.3a) collects all the control objectives of the closed-loop system, taking the name *multiobjective cost function*. In general form, (15.3a) can be written as:

$$J(\tilde{\mathbf{x}}, \tilde{\mathbf{u}}) = \sum_{i=0}^{n_J} \sum_{k=0}^{N} J_i(k), \tag{15.5}$$

where $n_J$ is the number of objectives and $J_{i,k}$ corresponds to the evaluation of each particular objective $i$ at time $k$. In the case of WTNs, (15.5) typically includes the objectives presented in Chapter 12.

### 15.2.3 Inclusion of fault-tolerant capabilities

The control problem $\langle \mathbb{O}, \mathbb{C}, \mathbb{U} \rangle$ described in Section 15.2.2 will now be reformulated to consider faults. If an active FTC strategy is considered, there are two main ways to adapt the MPC law to introduce fault tolerance [1]:

1. *System reconfiguration*. This consists of finding a new set of constraints $\mathbb{C}_f(\Theta_f)$, where $\Theta_f$ is the set of parameters changed by the faults such that the control problem $\langle \mathbb{O}, \mathbb{C}_f(\Theta_f), \mathbb{U}_f \rangle$ can be solved. This strategy can be applied when the fault detection and isolation (FDI) module does not provide a fault estimation. The faulty components are therefore unplugged by the supervisory system and the control objectives are achieved using non-faulty components. In the case of the actuators, this implies that the model (15.1) used by the MPC controller is modified as follows:

$$\mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k) + \sum_{i \in I_N} \mathbf{B}_i \mathbf{u}(k,i) + \mathbf{B}_d \mathbf{d}(k), \tag{15.6}$$

$$\mathbf{0} = \sum_{i \in I_N} \mathbf{E}_{u,i}\mathbf{u}(k,i) + \mathbf{E}_d\mathbf{d}(k), \tag{15.7}$$

where $I_N$ is the subset of non-faulty actuators.

2. *Fault accommodation*. This approach consists of solving the control problem $\langle \mathbb{O}, \hat{\mathbb{C}}_f(\hat{\Theta}_f), \hat{\mathbb{U}}_f \rangle$, where $\hat{\mathbb{C}}_f(\hat{\Theta}_f)$ is an estimate of current system constraints and parameters provided by the FDI module. This strategy can be applied when a change occurs in either system structure or parameters. In this strategy, the control law is modified while the remaining elements within the control loop are kept unchanged. In the case of the actuators, this requires that the system model (15.1) used by the MPC controller should be modified as follows:

$$\mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k) + \sum_{i \in I_N} \mathbf{B}_i\mathbf{u}(k,i) + \sum_{i \in I_F} \beta_i(\mathbf{u}(k,i), \theta_i) + \mathbf{B}_d\mathbf{d}(k), \tag{15.8}$$

$$\mathbf{0} = \sum_{i \in I_N} \mathbf{E}_{u,i}\mathbf{u}(k,i) + \sum_{i \in I_F} \varepsilon_i(\mathbf{u}(k,i), \theta_i) + \mathbf{E}_d\mathbf{d}(k), \tag{15.9}$$

where the functions $\beta_i$ and $\varepsilon_i$ and the parameters $\theta_i$ should be estimated by the FDI module for actuators belonging to the faulty actuator subset $I_F$.

Note that, in changing the model (15.1) of the MPC controller using either of the two previous strategies, the controller will consider the effect of the fault in the system model when computing the control action $\mathbf{u}^*(0|k)$. According to [9], this is different from other control laws (e.g., LQR, pole placement), where the control law should be designed off-line for the considered set of faults, so as to produce a bank of controllers that should be gain-scheduled on-line according to the fault features. However, depending on how critical the fault is, the MPC controller will not be able to compute a control input or else the computed control input will not lead to acceptable performance. For this reason, when using an MPC controller the effect of the fault and the admissibility of the obtained control input needs to be evaluated.

## 15.3 Proposed approach

This section describes a series of analyses to assess the fault-tolerance capabilities of the system after a fault has occurred and before applying a reconfiguration or accommodation strategy to achieve fault tolerance.

In case that a fault occurs, then:

- The system might have lost some of the properties required to proceed with system control, or
- That system performance is degraded to an unacceptable level and it is not worth continuing with system control by activating fault-tolerant strategies.

### *15.3.1 Admissibility analysis algorithms*

Before starting to apply the FTC strategies described above, it should be evaluated whether the MPC controller will be able to continue operating after fault occurrence. This is done by means of a set of admissibility analysis algorithms, which are based on a structural analysis to determine the loss of post-fault controllability, complemented by a feasibility analysis of the optimization problem related to the MPC design so as to consider the effect of the fault on actuator constraints. Moreover, by evaluating the admissibility of the different AFCs, critical actuators regarding fault tolerance can be identified considering structural, feasibility, performance and reliability analyses.

Let $I$ be the set of system actuators. The different admissibility analysis algorithms consider that the set of all subsets of system actuators is denoted by $2^I$. For each subset $K \subseteq I$, corresponding to a given AFC, and using the reconfiguration (or accommodation) approach described in Section 15.2.3, the algorithms evaluate whether or not a given system property, denoted by $P(K)$, is satisfied [1]. Thus,

$$P_K = \begin{cases} 1 \text{ if the property is satisfied,} \\ 0 \text{ if the property is not satisfied.} \end{cases} \tag{15.10}$$

This evaluation induces the set of all subsets of $I$, $2^I$, to be partitioned in two classes as follows:

$$2^{I+} = \{K \subseteq I; P_K = 1\}, \tag{15.11}$$

$$2^{I-} = \{K \subset I; P_K = 0\}. \tag{15.12}$$

The class $2^{I+}$ contains all the subsets of the actuators for which $P_K$ is satisfied. Thus, the admissibility analysis mainly aims to identify the following (see Figure 15.1):

- *Critical actuators*, i.e., the set of actuators that are required to satisfy $P_K$. For every analysis in Figure 15.2, a set of critical actuators will be identified.
- *Redundant actuators*, i.e., the actuators that are not critical for correct functioning of the system. These may be excluded as $P_K$ will continue to be satisfied.
- *Redundancy degree*, consisting of the number of extra non-critical actuators through which $P_K$ could hold. There are two types of redundancy: *weak* (corresponding to the largest number of sequential faults that can be tolerated in the best case scenario, i.e, while continuing to satisfy $P_K$) and *strong* (corresponding to the smallest number of sequential faults that can be tolerated in the worst case scenario).

The approach proposed here consists of a set of analyses based on both the graph and the mathematical model of the system (see Figure 15.2):

- From the system graph, the *structural analysis* allows to determine whether or not the system with a given AFC is structurally controllable. It does this by checking the existence of at least one path linking demands with sources. At this stage,

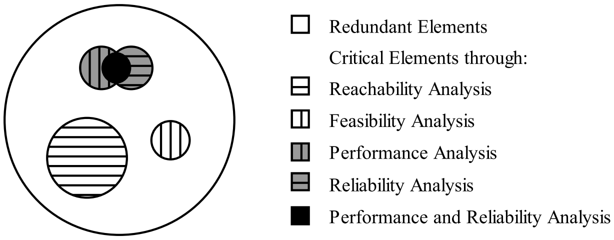

**Fig. 15.1** Critical and redundant actuators of the system

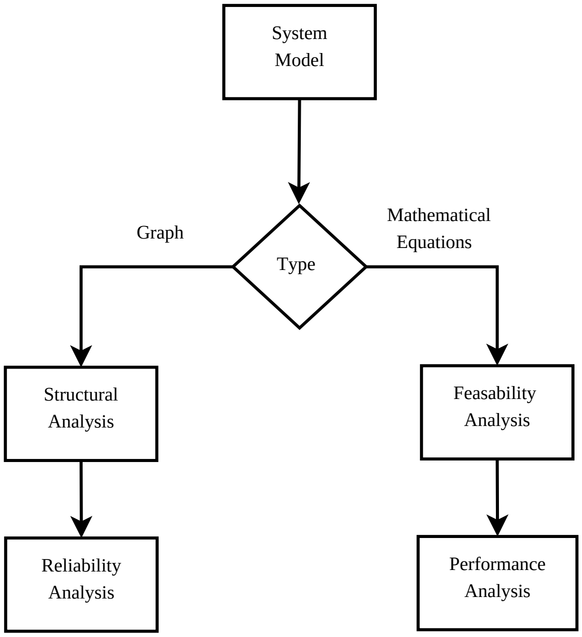

**Fig. 15.2** Flow diagram of the proposed actuator fault-tolerance evaluation approach

all possible paths linking demands and sources are also determined. Using this information, the *reliability* of the AFC can also be evaluated.

- From the system mathematical model, a constraint satisfaction problem (CSP) can be formulated that allows a *feasibility analysis* to be performed. This analysis allows the physical capacity of the system to be checked considering constraints in actuators and states (see (15.3a)). Moreover, as a complementary analysis, the *closed-loop performance* based on a given global objective for the AFC can be evaluated.

These two sets of analyses are complementary. When a reconfiguration strategy is used, connectivity between demands and sources may be lost when the faulty actuator is removed (see Section 15.2.3). This will affect both controllability and reliability. However, those properties do not take into account the physical limitations of the system actuators. Hence, although connectivity is preserved, the MPC-related optimization problem might lead to an unfeasible solution, due either to the lack of capacity of the remaining actuators or the poor performance of the control loop. This happens when an accommodation strategy is used, since although the connectivity among elements is preserved (the faulty actuator is not removed), the resulting MPC-related optimization problem may be unfeasible or the closed-loop control scheme may perform poorly.

As a result of the application of the methodology presented in Figure 15.2, it is possible to determine critical actuators as follows (type of analysis in brackets):

- Actuators that are essential to preserving demand-source connectivity (by means of structural controllability analysis).
- Actuators that are indispensable to preserving the capacity to move the desired water volume from sources to meet demands taking into account actuator physical constraints (by means of structural controllability analysis).
- Actuators whose malfunction generates high suboptimality of the considered control objective if the system is maintained in operation after fault detection (by means of performance analysis).
- Actuators whose malfunction does not guarantee reliable operation of the system (by means of reliability analysis).

Figure 15.1 depicts the different types of critical actuators that can be identified applying the sequence of analyses presented in Figure 15.2. Results for each analysis are considered in subsequent analyses, in such a way that actuators that are considered critical at a given stage of the methodology might not be further considered in later analyses.

### *15.3.2 Analyses based on the system graph*

The structural analysis algorithm copes with connectivity properties of the system without considering the actual value of the model parameters or the limitations of the actuators[7]. This test is used to evaluate the admissibility of a given AFC when the reconfiguration FTC strategy is used, i.e., when an actuator is removed after fault occurrence and the system is controlled by the remaining actuators.

The algorithm starts by determining the digraph[8] $G(\mathcal{V},\mathcal{E})$ of the model used for the MPC controller. Using the digraph, the *structural controllability* of the system for a given AFC will be evaluated. If this property is preserved after the actuator fails, the AFC is admissible, i.e., it is able to tolerate the fault; otherwise, the AFC is not admissible. To evaluate structural controllability from the system graph, some basic graph theory concepts will be used (see [2] for more details). Using Theorems

[7] See [1] for important definitions related to the topic.

[8] See [22] for details on how to obtain a digraph from the system model.

**Algorithm 9** Controllability analysis using the structural approach

```
Obtain the digraph $G = (\mathcal{V}, \mathcal{E})$ of the system model used for designing the MPC (related to the
  optimization problem in (15.3a)) given a particular AFC
From the system digraph $G = (\mathcal{V}, \mathcal{E})$, find the reachability matrix $\Gamma$
for each $\mathbf{x}_i \in \mathbb{R}^{n_x}, i = 1, \ldots, n_x$ do
    if $\nexists \mathbf{u}_j \in \mathbb{R}^{n_u}, j = 1, \ldots, n_u \mid \Gamma_{ij} = 1$ then
        AFC is non input-reachable
    else
        if s-rank([A B]) $\neq n$ then
            is non-structurally controllable
        else
            is structurally controllable
        end if
    end if
end for
```

1 and 2, Algorithm 9 will perform the structural controllability analysis for a given AFC.

## *15.3.3 Analyses based on the system mathematical model*

### Feasibility analysis algorithm

To evaluate the admissibility of the control of a given AFC when system constraints (15.2) are considered, it is not possible to use the structural analysis algorithm[9]. presented in Section 15.3.2.

Feasibility in an MPC controller design is a key property to be satisfied before the control action can be computed by solving the optimization problem (15.3a) [9]. In this case, the admissibility evaluation problem for a given AFC can be naturally handled as a CSP. Consequently, the feasibility evaluation of the MPC-related optimization problem (here for a given AFC using the reconfiguration strategy)[10] can be checked using Algorithm 10.

### Performance analysis algorithm

The degradation of the control objective in a faulty situation can be quantified by means of maximal loss of efficiency $\rho$ with respect to the objective function in a non-faulty situation $J_0$. This fact establishes whether of not the control objective

[9] This would also be the case when an accommodation FTC strategy is used, since the actuator would not be removed after the fault but would be operated under the remaining operating range estimated by the FDI module.

[10] In case that an accommodation strategy is used, the faulty model used in Algorithm 10 should be replaced by the one used in (15.8).

**Algorithm 10** Feasibility Analysis

```
1: for $k$ = 1 to $H_p$ do
2:     $\mathcal{U}(k-1) \Leftarrow \mathcal{U}$
3:     $\mathcal{X}(k) \Leftarrow \mathcal{X}$
4: end for
5: $\mathcal{W} \Leftarrow \{\overbrace{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{H_p}}^{\tilde{\mathbf{x}}}, \overbrace{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{H_p-1}}^{\tilde{\mathbf{u}}}\}$
6: $\mathcal{D} \Leftarrow \left\{\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_{H_p}, \mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_{H_p-1}\right\}$
7: $\mathcal{Z} \Leftarrow \left\{ \left( \mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k) + \sum_{i \in I_N} \mathbf{B}_i \mathbf{u}(k,i) + \mathbf{B}_d \mathbf{d}(k), \quad \mathbf{0} = \mathbf{E}_u \mathbf{u}(k) + \mathbf{E}_d \mathbf{d}(k) \right)_{k=0}^{H_p-1} \right\}$
8: $\mathcal{H}_{\mathcal{A}} = (\mathcal{W}, \mathcal{D}, \mathcal{Z})$
9: if the CSP $\mathcal{H}_{\mathcal{A}}$ has solution then
10:     AFC is admissible
11: else
12:     AFC is non-admissible
13: end if
```

degradation after an actuator fault $J_f$ is admissible. Thus, an AFC is admissible regarding performance if the following condition is satisfied: $J_f \leq (1+\rho)J_0$. This condition will enable a performance analysis of the AFC considering the faulty actuator, with either an accommodation or a reconfiguration strategy.

The procedure for evaluating the performance admissibility of the controller with respect to the fault situation is summarized by Algorithm 10, modifying the constraints defined in step 7 to add a new constraint:

$$\phi_{x_{H_p}} + \sum_{i=0}^{H_p-1} \Phi_i(\mathbf{x}_i, \mathbf{u}_i) \leq (1+\rho)J_0. \tag{15.13}$$

Notice that, as in the case of the feasibility analysis, the existence of a solution to the CSP associated with MPC performance evaluation for a given AFC using the reconfiguration strategy[11] can be proved by Algorithm 10 but including the new constraint (15.13), which considers the admissibility condition with respect to control performance over the prediction horizon $H_p$ stated in the MPC controller.

### *15.3.4 Reliability analysis algorithm*

Reliability is defined as the probability that a given component (or system) will accomplish its intended function during a given period of time and in specific operating conditions and environments [6]. In other words, it is the probability of success in accomplishing a task or achieving a desired property in a process, based on proper

[11] If an accommodation strategy is used, the fault model used in Algorithm 10 should be replaced by the one used in (15.8).

operation of components. The main advantages of including a reliability analysis are as follows:

- Information on component health is integrated in controller design and improves the life of the system components
- Reliability information on the system can be considered as design criteria to be used in MPC implementation including FTC capabilities
- Essential actuators whose malfunction causes abrupt system reliability decay are identified.

In the case of WTNs, reliability is understood as the ability of the network to provide an efficient water supply to consumers under both normal and abnormal operating conditions. For this reason, reliability is a measure of WTN performance. Reliability in WTNs has already been considered in the literature [14, 25].

When a reconfiguration FTC strategy is used, the reliability of DTWNs can be affected due to the probabilities of success of each of the components in the new configuration. For this case, the admissibility evaluation problem of a given AFC can be handled as composite reliability of the subsystems in the system. In particular, since reliability in DTWNs is related to guaranteed supply to consumers, it can be determined based on all the possible paths linking demands and sources from the network graph already obtained in the structural analysis.

The global reliability of a system, denoted by $R_{g,k}$, generally consists of the decomposition of its subsystems into elementary combinations of serial and parallel subsystems that can be extracted from the matrix containing all paths linking demands and sources [7]:

- Reliability of $n_p$ parallel subsystems is defined as:

$$R_p(k) = 1 - \prod_{i=1}^{n_p} (1 - R_i(k)). \tag{15.14}$$

- Reliability of $n_s$ serial subsystems is defined as:

$$R_s(k) = \prod_{i=1}^{n_s} R_i(k), \tag{15.15}$$

where $R_i(k)$ represents the reliability of the $i$-th actuator (or subsystem) at time $k$ and where $\gamma_i(k)$ is the failure rate modelled as an exponential distribution

$$R_i(k) = e^{-k\gamma_i(k)}. \tag{15.16}$$

Thus, overall system reliability is given by

$$R_g(k) = \prod_{i=1}^{n_s} (1 - \prod_{i=1}^{n_p} (1 - R_i(k))). \tag{15.17}$$

**Algorithm 11** Reliability analysis

```
Decompose the system in $n_p$ parallel subsystems and $n_s$ subsystems using the system graph.
for $i = 1$ to $n_u$ do
    Evaluate actuator reliability $R_i(k)$ using (15.16).
end for
for $g = 1$ to $n_p$ do
    Evaluate reliability of parallel subsystems $R_{p,k}$ using (15.14) and (15.16).
end for
for $g = 1$ to $n_s$ do
    Evaluate reliability of system $R_g(k)$ using (15.17) and the result obtained from the evaluation
    in (15.14).
end for
```

Algorithm 11 shows the reliability evaluation of a given AFC based on computing system reliability. Since the calculation of reliability for each and every AFC could impose a great computational burden, to save time, the path matrix that contains all the possible paths in the system graph is used. This matrix has the following structure:

$$\begin{array}{c|c|c|c|c|c|}
 & p_1 & p_2 & p_3 & \dots & p_{n_{ph}} \\
\hline
u_1 & 1 & 0 & 1 & \dots & 0 \\
u_2 & 0 & 1 & 1 & \dots & 1 \\
u_3 & 1 & 0 & 0 & \dots & 1 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
u_{n_u} & 0 & 1 & 1 & \dots & 1
\end{array} \tag{15.18}$$

where $n_{ph}$ is the number of path and 1 and 0 indicate the presence and absence, respectively, of an actuator in the path. Each time a component malfunctions, the row assigned to that actuator is withdrawn along with all the paths that make use of it. To evaluate fault tolerance for the rest of the system, the reliability index $R_g(k)$ should be greater than a specific admissibility threshold $R_{th}$ at a given time horizon $k_{end}$, both defined by the user.

### *15.3.5 MPC redesign to preserve reliability*

When a fault occurs, the MPC law is modified to cope with the fault, as discussed in Section 15.2.3. As explained in [7], the value of the actuator failure rate changes because the control action should be increased in order to compensate for the fault effect. In this case, energy consumption increases and the value of the failure rate also increases due to the actuator load increment. Thus, there is an interplay between maintaining closed-loop performance and reliability. To maintain the desired performance, the relationship between the actuator load increment and reliability can be established. One of the most commonly used relationships is based on assuming that the actuator failure rate changes with the load through the following exponential law:

$$\gamma_i(k) = \gamma_i^o e^{\beta_i \mathbf{u}_i(k)}, \tag{15.19}$$

where $\gamma_i^o$ represents the baseline failure rate (nominal failure rate) and $\mathbf{u}_i$ is the control action for the i-$th$ actuator. Parameter $\beta_i$ is a fixed factor that depends on the actuator characteristics. Thus, the reliability of the actuator can be expressed in terms of its load as follows:

$$R_i(k) = e^{k\gamma_i} = e^{\gamma_i^o e^{k\beta_i \mathbf{u}_i(k)}}. \tag{15.20}$$

Consider that a predefined reliability threshold $R_{th}$ should be maintained until the end of the system mission at time $k_{end}$. This threshold defines the minimal acceptable reliability value in the degraded fault mode. The aim is to translate this threshold to a load threshold that can be applied to the actuator. This actuator load threshold can be derived from (15.20) as follows:

$$|u_{i,th}| = \frac{1}{\beta_i} \ln\left(\frac{\ln R_{i,th}}{\gamma_i^o k_{end}}\right). \tag{15.21}$$

Hence, the MPC controller (15.3a) can be redesigned by including the following constraint in the i-$th$ actuator control:

$$u_i \in \left[-u_{i,th}, u_{i,th}\right]. \tag{15.22}$$

However, as discussed in [27], this will only preserve the reliability of the i-$th$ actuator. In order to preserve the reliability of the whole WTN, the new actuator constraints (15.22) should be derived taking into account the reliability expression (15.15) and the reliability threshold $R_{th}$ at the end of the MPC prediction horizon $H_p$. This can be achieved by formulating a CSP problem, such as that reflected in Algorithm 12, which considers, as constraints, the reliability of the WTN in (15.15) derived by means of Algorithm 11 in terms of the reliability of each actuator, the impact of actuator load (see (15.20)) and the actuator operational constraints defined in (15.3a).

After solving the CSP problem in Algorithm 12, to solve the optimization problem associated the MPC design, the resulting updated actuator constraints are used instead of the actuator operational constraints defined in (15.3a). In this way, it can be guaranteed that the MPC controller computes a control sequence that preserves reliability. There is, of course, a trade-off between reliability and performance. Increasing the reliability threshold $R_{th}$ will imply a reduction in the WTN performance but will extend the life of the remaining actuators.

**Algorithm 12** MPC redesign to preserve reliability

```
for $k = 1$ to $H_p$ do
    $\mathcal{U}(k-1) \Leftarrow \mathcal{U}$
end for
$\mathcal{W} \Leftarrow \{\overbrace{\mathbf{u}_1, u_2, \ldots, \mathbf{u}_{H_p-1}}^{\tilde{\mathbf{u}}}\}$
$\mathcal{D} \Leftarrow \left\{\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_{H_p-1}\right\}$
$\mathcal{Z} \Leftarrow \left\{\left(R_g(k) = f(R_i(k)), R_i(k) = e^{\gamma_i^o e^{k\beta_i|u_i|}}, i = 1, \ldots, n_u\right)_{k=0}^{H_p-1}, R_g(H_p-1) > R_{th}\right\}$
$\mathcal{H}_{\mathcal{A}} = (\mathcal{W}, \mathcal{D}, \mathcal{Z})$
$\left\{\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_{H_p-1}\right\} \Leftarrow$ solve$(\mathcal{H}_{\mathcal{A}})$
```

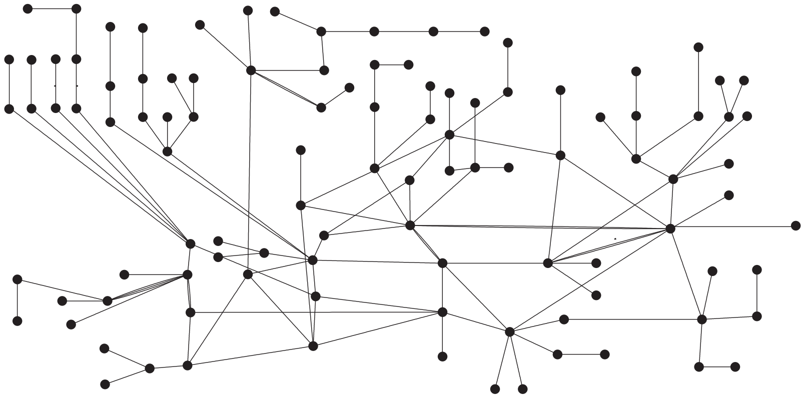

**Fig. 15.3** Graph of the Barcelona WTN

## 15.4 Simulations and results

### 15.4.1 Case study description

The Barcelona WTN, presented in Figures 2.2, 2.3 and 2.4 of Chapter 2), is used as the case study of this chapter. Figure 15.3 shows the graph derived from this network; the nodes correspond to reservoirs or pipe merging/splitting nodes and the arcs correspond to actuators (valves and pumps). Five of the pumps are used to draw water from underground sources and the remaining pumps satisfy water demand at appropriate pressure levels. The network has 88 main water consumption sectors (for further information regarding the Barcelona WTN, see [15]). Both the demand episode and the calibration set-up of the network are as established by Aguas de Barcelona. The control centre has a telecontrol system for network management. The Barcelona WTN also has some 98 remote stations, which manage about 450 elements in real time, including flow meters, pumps, valves and chlorine dosing instruments.

The system control objective set for the MPC controller is to minimize operational costs (water transport and production for the entire network) while satisfying water demand for each consumption sector [15]. Thus, recapping on Chapter 12, the economic objective function can be written as follows:

$$J(k) = \sum_{i=0}^{H_p-1} [\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2(k)]\mathbf{u}(k), \tag{15.23}$$

which takes into account the water cost $\boldsymbol{\alpha}_1$ (price of water at source) and the electricity cost $\boldsymbol{\alpha}_2(k)$ (operation of pumps and valves). Note that the time variance of $\boldsymbol{\alpha}_2$ is due to the fact that pumping costs vary according to the time of day. The prediction horizon $H_p$ is 24 hours. No terminal cost is considered in this application.

Demands are imposed as equality constraints in the model (15.1) used by the MPC controller, which, in the case of the WTN, can be expressed in discrete-time state-space form (15.1) using a sampling time $\Delta t = 1$ hour. Moreover, $\mathbf{x} \in \mathcal{X} \subseteq \mathbb{R}^{n_x}$ is the state vector corresponding to the water volumes of the $n_x = 63$ tanks, $\mathbf{u} \in \mathcal{U} \subseteq \mathbb{R}^{n_u}$ represents the vector of manipulated flows through the $n_u = 130$ actuators (pumps and valves) and $\mathbf{d} \in \mathcal{D} \subseteq \mathbb{R}^{n_d}$ corresponds to the vector of the $n_d = 88$ water demands (consumption sectors).

There are 16 nodes in the Barcelona WTN and since demand can be forecasted, these are assumed to be known. Thus, **d** is a known vector of non-negative elements that contains the measured disturbances (demands) affecting the system.

### *15.4.2 Results*

Several tests and analyses were performed for the Barcelona WTN case study to illustrate the proposed methodology. Figure 15.2 shows the sequence of tests applied. In this section, all the capabilities of each analysis are explored, while Section 15.4.3 describes only the ones necessary for this study. The results were obtained using a 1.5 GHz and 2.00 Gb RAM Intel(R) Core(TM)2 Duo PC . Matlab$^{©}$ and Tomlab were used to perform the simulations.

The structural analysis was carried out using the computed *reachability matrix* and *path computation*, which, as expected, produced equivalent results. However, each technique yielded several additional results that provided important information concerning to the operation and behaviour of the WTN. From the reachability analysis, it is possible to determine which states were structurally controllable, while the path computation analysis obtained all possible paths from a source to a destination node as well as, for each path, an approximate operational cost (according to the electricity cost of each element) and a maximal water flow (according to the physical constraints of the actuators). In this stage, critical actuators were located and different approaches were used according to the applied strategy. Although a fault scenario with a faulty actuator at each time instant was considered in both cases, the representation of the malfunction was denoted in different ways. In the reachability analysis, the malfunction was determined from the state-space matrices (a zero value was forced in the position where a connection value previously existed between the state and the actuator failure). In path computation, all paths with the faulty component were extracted from the path matrix (15.18). From this study, the critical actuators for each state and for the whole network could be identified. Note that although the results obtained by both techniques in the structural analysis were similar, the computation time required for the reachability-matrix-based strategy was much higher, at almost 200 times the time consumed by the path computation technique (579 s vs. 3 s).

The feasibility analysis can only be implemented if the previous analysis is first made, since its implementation is based on the path matrix calculation. The result of this analysis was a set of paths that guaranteed that demand was satisfied, taking into account the physical constraints of the network actuators. The cost of maintaining correct network operations was also obtained in this stage. The time consumed by this analysis was 1.57 s.

Performance was computed using the objective function (15.23) and the actuator constraints. The analyses were performed taking into account faulty components and comparing the corresponding performance with the fully operative case (non-faulty system). The computation time needed for this analysis was 8 s. Finally, the reliability analysis showed the level of reliability of each component and path and of the whole network. AFCs were analysed by extracting all paths using the faulty actuator and re-computing the reliability of the WTN. Two rankings were computed: the first one according to demand satisfaction, showing which demands were more likely to be unsatisfied; and the second one according to the most critical actuators, showing how the reliability of the entire network decreased if those actuators were damaged. The computation time in this case was 5 s.

### *15.4.3 Discussion*

Although each of the previous analyses can individually provide a great deal of information about the fault tolerance of a network, linking them up reduces the computational burden. In order to clearly present and easily discuss the proposed methodologies, a smaller portion of the Barcelona WTN (see Figure 15.4) was used for illustrative purposes.

The first test consisted of locating the critical network actuators by means of a structural analysis. These critical actuators are those without which (outage) path connectivity is lost. The results of this analysis, summarized in Tables 15.1 and 15.2, point to an important number of critical actuators within the network, due to the topology and the way of connecting network elements, as most actuators (valves or pumps) are the only link between tanks and demands. Therefore, if an actuator fails, then the corresponding demand will not be satisfied. Note that the information shown in Tables 15.1 and 15.2 is particularly significant for Aguas de Barcelona (the manager of the water infrastructure), since it identifies the critical elements in

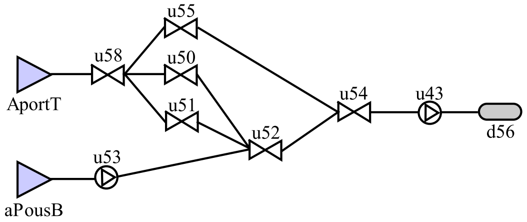

**Fig. 15.4** Portion of the WTN related to Demand 56

**Table 15.1** Structural Critical Actuators (towards tanks)

| No. | Name | No. | Name | No. | Name | No. | Name |
|---|---|---|---|---|---|---|---|
| 122 | iAltures | 15 | iCanGuey2 | 62 | iGuinardera1 | 30 | iPapiol1 |
| 10 | iBegues1 | 14 | iCanGuey3 | 60 | iGuinardera2 | 88 | iSJD10 |
| 6 | iBegues2 | 21 | iCanRoig | 101 | iLaSentiu | 7 | iStBoi |
| 2 | iBegues3 | 57 | iCanRuti | 34 | iMasGuimbau1 | 9 | iStCliment1 |
| 1 | iBegues4 | 37 | iCarmel | 31 | iMasGuimbau2 | 5 | iStCliment2 |
| 32 | iBellsoleig | 43 | iCerdMontflorit | 100 | iMasJove | 40 | iStGenis1 |
| 61 | iBonavista | 42 | iCerdUAB | 68 | iMntjcStaAmalia | 38 | iStGenis2 |
| 20 | iCanGuell1 | 12 | iCesalpina1 | 69 | iMntjcTresPins | 13 | iStaClmCervello |
| 17 | iCanGuell2d3 | 11 | iCesalpina2 | 3 | iOrioles | 45 | iStaMaMontcada |
| 16 | iCanGuell2d5 | 82 | iCornella100 | 23 | iPalleja1 | 35 | iTibidabo |
| 18 | iCanGuey1d2 | 39 | iFlorMaig | 24 | iPalleja2 | 56 | iTorreBaro1 |
| 19 | iCanGuey1d5 | 109 | iFnestrelles300 | 27 | vPalleja70 | 65 | iTorreoCastell |
| 44 | iVallensana1 | 8 | iViladecans1 | 4 | iViladecans2 | 25 | vAbrera |
| 54 | vCerdanyola90 | 63 | vMontigala | 90 | vSJD | 59 | vTerStaColoma |
| 104 | vSJDTot | 58 | vTer | | | | |

the network for surveillance/correction policies to be implemented in the event of element damage (fault).

**Table 15.2** Structural Critical Actuators (towards demands)

| No. | Name | No. | Name | No. | Name | No. | Name |
|---|---|---|---|---|---|---|---|
| 115 | vPallejaATLL | 116 | iPalleja3 | 117 | iMasGuimbau3 | 118 | iVallvidrera |
| 119 | vHorta | 120 | iUAB | 121 | iVallensana2 | 122 | iBoscVilaro |
| 123 | iTorreBaro2 | 124 | iCerdSabadell | 125 | vBesosStaColoma | 126 | v117Montigala |
| 127 | v70CFE | 128 | v55BAR | 129 | iMontemar | 130 | vAltures |

Applying the first test to the network, as depicted in Figure 15.4, four possible paths were detected. These were:

Path 1: $AportT \rightarrow u58 \rightarrow u50 \rightarrow u52 \rightarrow u54 \rightarrow u43 \rightarrow d56$
Path 2: $AportT \rightarrow u58 \rightarrow u51 \rightarrow u52 \rightarrow u54 \rightarrow u43 \rightarrow d56$
Path 3: $AportT \rightarrow u58 \rightarrow u55 \rightarrow u54 \rightarrow u43 \rightarrow d56$
Path 4: $aPousB \rightarrow u53 \rightarrow u52 \rightarrow u54 \rightarrow u43 \rightarrow d56$

Analysing the structure of the network, as depicted in Figure 15.4, it can be observed that it contains two critical actuators: 54 and 43. If either of these actuators fail, then Demand 56 will not be satisfied. All the remaining actuators can be considered as redundant actuators.

The second analysis done to the Barcelona WTN was to identify the actuators whose physical constraints limit water transport capacity through a certain path. Note that this analysis did not consider any fault in those actuators. The analysis, performed using Algorithm 10, also pinpointed several alternative paths through which water transport is possible (or even mandatory) given the constraints of the paths for supplying demands.

Results for this last analysis considering the whole WTN identified other critical actuators: 26, 52 and 91 (namely *iPalleja4, vBesosMontCerd* and *vGava100a80*. Note that the increase in the number of critical actuators, taking into account their physical constraints, is not significant. For the network in Figure 15.4, actuator 52 is not a critical element according to the structural controllability property, meaning that connectivity is not lost when this component fails. However, the feasibility analysis determined that this actuator was in fact critical when the actuator physical constraints were considered. Actuator 52 cooperates with a flow of water to satisfy the demand that cannot be satisfied with a flow through a single path.

The third analysis identified the optimal paths to reach a selected destination node without considering the system constraints, i.e., the *structural optimal paths*. This analysis was performed using the structural algorithm, as explained in Section 15.3.2. For the smaller network the cost of each path was computed, corresponding to the electricity cost of the actuators for both paths and the cost of water treatment in a determined source. For paths 1, 2 and 3, the cost was 0.54 e.u.[12], while for path 4 the cost was 0.77 e.u. This small example would indicate that any of the first three paths is optimal for satisfying Demand 56.

A criterion to decide which of the three paths is optimal for this demand is to calculate the maximum flow of water for each path, which can also be computed in this analysis and is given by the smallest value of the maximum flow of water of the actuators in a given path. In this case, since all paths were restricted to 0.3 $\mathrm{m}^3$/s, due to the physical capacities of actuator 43, any of the first three paths are recommended. However, if actuator 43 were not considered, path 1 would be the optimal path as it has a maximum flow of 2.2 $\mathrm{m}^3$/s, while in the other paths, actuator 55 is restricted to 0.35 $\mathrm{m}^3$/s, and actuators 51 and 52 to 0.8 $\mathrm{m}^3$/s.

[12] Note that costs are given in *economic units* (e.u.) rather than real units (€) for confidentiality reasons.

**Table 15.3** Entire WTN Performance Analysis

| Actuator No. | Faulty cost [e.u.] | Cost overrun [%] |
|---|---|---|
| 41 | 514.44 | 2.43 |
| 47 | 515.94 | 2.73 |
| 74 | 528.05 | 5.14 |
| 78 | 557.62 | 11.03 |
| 86 | 515.08 | 2.55 |
| 89 | 556.22 | 10.74 |
| 97 | 510.49 | 1.64 |
| 102 | 539.87 | 7.49 |
| 103 | 552.21 | 9.95 |

The fourth analysis consisted of identifying the set of optimal paths including the objective function (15.23) and the system constraints (15.2a)-(15.2b). Path details are not provided here, but the total costs of maintaining the whole DTWN in proper working order and satisfying all its demands was 502.25 e.u. In the case of the network depicted in Figure 15.4, the optimal path obtained from the fourth analysis was path 4. Although it may appear that, when only Demand 56 is considered without the interconnection of the entire network, the other paths are less costly when the entire network is considered, this is not true. The actuators used in path 4 are also used to satisfy other demands, so sharing components results in an optimal solution.

The fifth test was performance analysis, taking into account the critical actuators already identified in the previous tests, with the difference in costs showing the impact that a single faulty actuator could have on an entire network. Results from this analysis are summarized in Table 15.3. Note that all comparisons took into account an optimal functioning cost (under non-faulty conditions) of 502.25 e.u. Moreover, fault cost denotes the functioning cost under faulty conditions.

According to the analysis of the entire WTN, some actuators did not have a significant impact on the total performing cost (e.g., actuators 28, 29, 33, 64, 71, 80, 81, 85, 87, 94, 107, 108, 113). However, other actuators (such as 78 or 89) significantly increased cost, taking into account daily estimates. These latter actuators are shown in Table 15.3. Degradation in costs obtained with this analysis can be the foundation for the introduction of redundant actuators in the network or an alternative fault tolerance strategy. For the network depicted in Figure 15.4, the performance analysis shows that the cost of maintaining operations for the network with a fault in any of these actuators does not increase the cost.

The accommodation and reconfiguration strategies presented in Section 15.2.3 are now illustrated for the case of a fault in actuator 108 (named *vTerMontcada*), which according to the previous analysis, is redundant. First the reconfiguration strategy is illustrated. Figure 15.5 presents the volume behaviour of tank 33, which

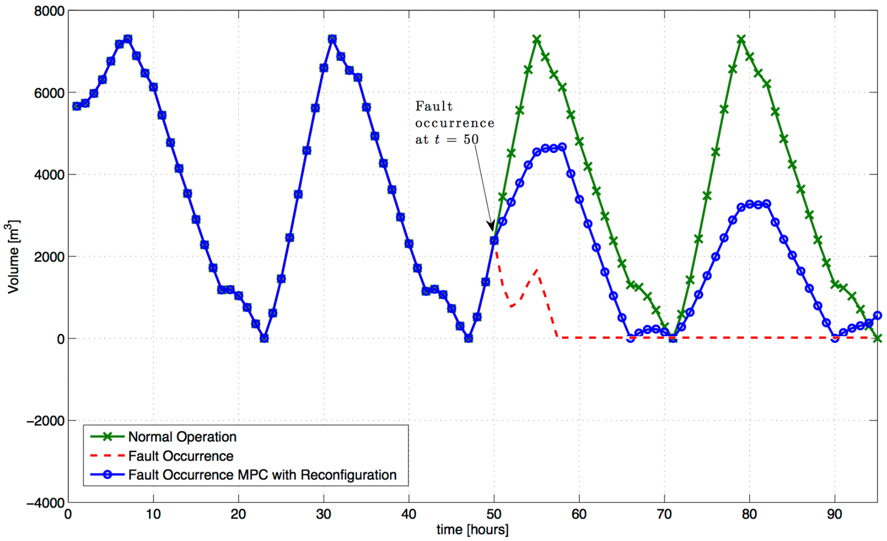

**Fig. 15.5** Volume evolution of Tank 33 with MPC using Reconfiguration

is supplied by two actuators: 73 (*iCornella130*) and 108 (*vTerMontcada*). It can be seen that in a non-faulty situation, the volume of this tank presents a repetitive pattern (filling when pumping is cheaper and emptying otherwise) to satisfy the water demand. However, when a fault occurs (at $k = 50$ hours), if the MPC controller is not reconfigured (labelled as fault occurrence in the plots), tank 73 volume drops to zero at $k = 58$ hours and demand is not satisfied anymore (unfeasible solution). However, if the MPC controller is reconfigured by removing the faulty actuator 108 from the control model, the tank level is still able to supply the required demand. However, the tank volume decreases with time, indicating that the faulty actuator should be repaired. Figures 15.6 and 15.7, which depict the behaviour of actuators 108 and 73, show that actuator 73 starts to deliver more flow in an effort to compensate for the faulty actuator 108 that is removed.

Figures 15.8, 15.9 and 15.10 depict tank 33 volume and actuator 108 and 73 flows when the fault is accommodated by the MPC controller. The fault affecting actuator 108 reduces the operating range by 50%. In this case, the faulty actuator is not removed from the control model of the MPC controller; rather, the operating limits of actuator 108 are updated according to the new operating range. Figure 15.8 shows how the volume behaviour of tank 33 in a non-fault situation and when using accommodation looks exactly the same; in contrast, when the controller is not accommodated, the volume tends to zero and demand is not satisfied.

From Figures 15.9 and 15.10, it can be seen that the MPC controller compensates for the reduction in the faulty actuator's operating range by increasing use of the non-faulty actuator, thereby compensating for the impact of the fault.

Although the proposed algorithm improves handling of the behaviour of the tank volume and actuator flows, it has computational and financial costs, as implementa-

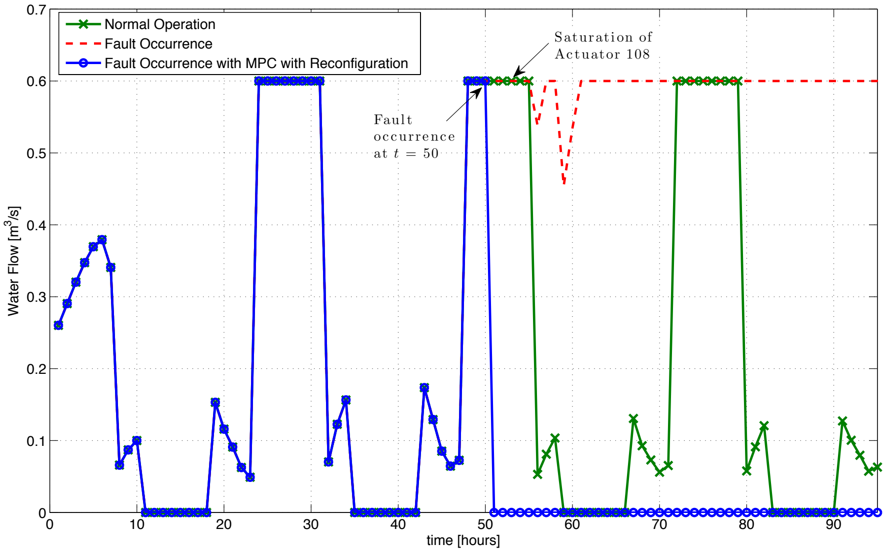

**Fig. 15.6** Water flow in Actuator 108 with MPC using Reconfiguration

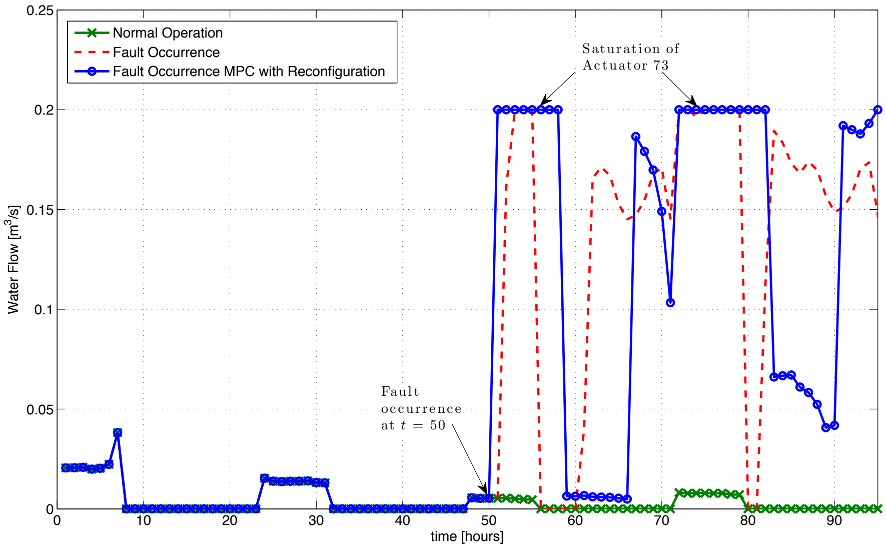

**Fig. 15.7** Water flow in Actuator 73 with MPC using Reconfiguration

tion of this feature increments computation time by 30 s (12%) and the cost overrun by around 9%.

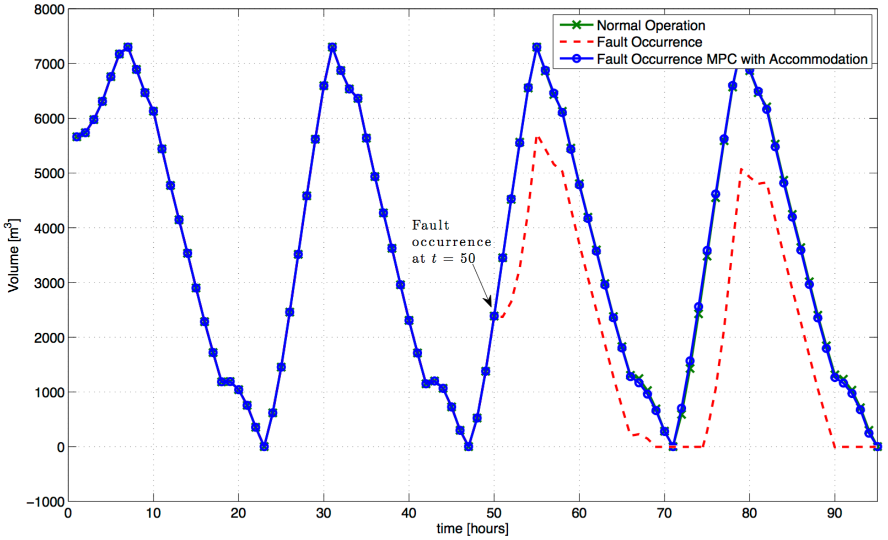

**Fig. 15.8** Evolution of volume in Tank 33 with MPC using Accommodation

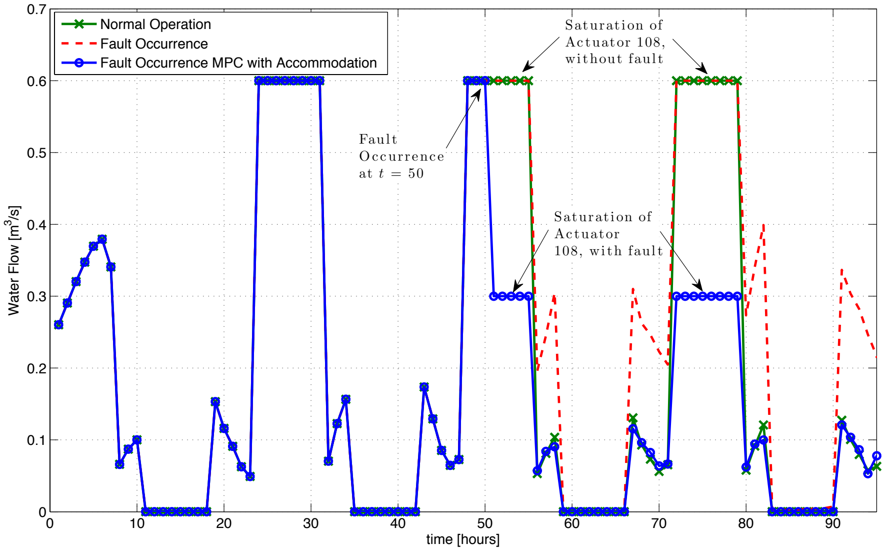

**Fig. 15.9** Water flow in Actuator 108 with MPC using Accommodation

The reliability analysis also takes into account the results of the previous analysis. The reliability of the entire network considering proper operation is 90.74% successful in satisfying the desired property when the reliability of each component is calculated using (15.16) with $\gamma = 0.0034$ (data obtained [10]). The association be-

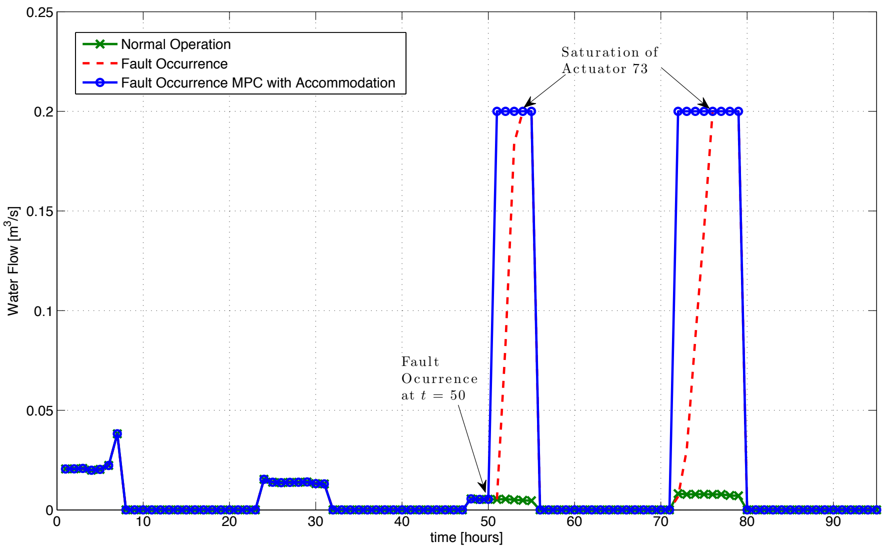

**Fig. 15.10** Water flow in Actuator 73 with MPC using Accommodation

**Table 15.4** Association between demand satisfaction and reliability

| **Demand No.** | **Percentage of total demand [%]** | **Faulty Components** | **$R_g^p$ in Faulty conditions [%]** |
|---|---|---|---|
| 69 | 9.1 | 128 | 0 |
| 83 | 4.0069 | 82, 88, 90, 104 | 0 |
| 70 | 3.2537 | 125 | 0 |
| 70 | 3.2537 | 58 | 99.33 |
| 70 | 3.2537 | 53, 50, 51 | 99.99 |
| 33 | 1.964 | 108 | 99.98 |
| 58 | 1.9407 | 52, 58 | 99.33 |
| 56 | 1.6777 | 52, 58 | 98.67 |
| 64 | 1.4941 | 58, 59 | 0 |

tween demand satisfaction and reduced reliability when a faulty component exists is shown in Table 15.4.

As can be seen in Table 15.4, although most faults in actuators do not significantly affect reliability in satisfying demand, some completely override the satisfaction of the desired property. These actuators are critical actuators regarding reliability. The risk of having a malfunction in the system can be better understood when

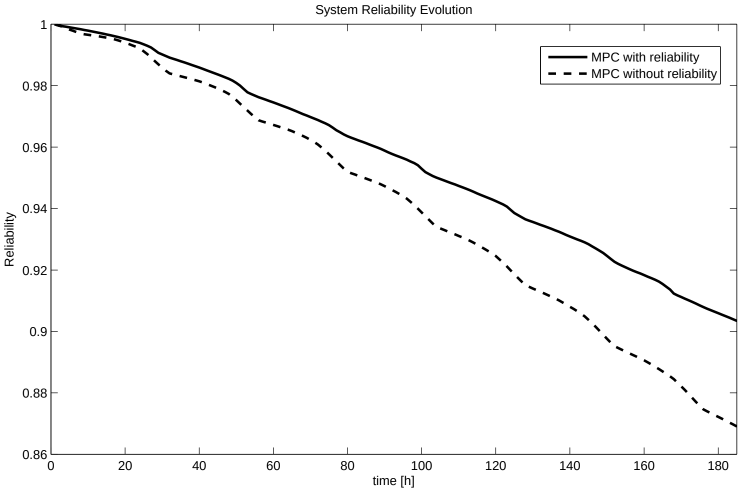

**Fig. 15.11** MPC redesign to preserve reliability

the reliability of the entire network is computed. Examples of critical actuators obtained from this study were actuators 102 and 103 since their malfunction led to a drop of 31.13% in the reliability of the entire network.

The reliability analysis was applied to the network depicted in Figure 15.4. The reliability of satisfying Demand 56 decreased to 1.33% if actuators 52 and 58 had a fault, highlighting the importance of both these actuators for the operation of this smaller network, and decreased to 0% when actuators 43 and 54 were faulty, reaffirming the fact that these two actuators are critical. Otherwise, reliability remained the same. Regarding the entire WTN, actuator 52 decreased reliability of satisfying the demands in the network by 21.71%, denoting again that it is an important element in system interconnectivity.

Critical actuators 43 and 54, when they malfunction, reduced the reliability of the entire system towards zero; in contrast, the fact that other actuators did not affect reliability denote them to be redundant actuators.

Finally, the MPC redesign approach to preserve the network reliability has been applied to the entire WTN using Algorithm 12. Figure 15.11 shows how the reliability of the network evolves in time when this algorithm is used. It can be observed that with the use of Algorithm 12, the reliability of the network degrades slowly compared to the case that the reliability is not considered in the MPC design.

## 15.5 Conclusions

This chapter has proposed a reliable fault-tolerant model predictive control strategy for drinking water transport networks. The proposed approach combines structural, feasibility, performance and reliability analyses. After a fault, the predictive controller is redesigned to cope with the fault by considering either a reconfiguration or an accommodation strategy depending on available knowledge regarding the fault. Before starting to apply the fault-tolerant control strategy, whether the predictive controller will be able to continue operating after the fault appearance needs to be evaluated. This evaluation is performed by means of a structural analysis to determine post-fault loss of controllability, complemented with a feasibility analysis of the optimization problem related to the predictive control design, so as to consider the fault impact on actuator constraints. By evaluating the admissibility of different actuator-fault configurations, critical actuators regarding fault tolerance can be identified. The proposed approach also allows for a degradation analysis of the system in terms of performance and reliability. As a result of this analysis, the predictive controller design can be modified by adapting constraints such that the best achievable performance with some pre-established level of reliability is achieved. The proposed approach, successfully tested on the Barcelona water network, shows that relevant information can be extracted about critical actuators considered in the different analyses. Future research will investigate the impact of uncertainty on the analyses and on the design of the predictive controller including fault-tolerant capabilities.

## References

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

[2] J.A. Bondy and U.S.R. Murty. *Graph Theory with Applications*. MacMillan Press, Great Britain, 1982.

[3] M.A. Brdys and B. Ulanicki. *Operational Control of Water Systems: Structures, Algorithms and Applications*. Prentice Hall International, 1994.

[4] E. F. Camacho, T. Alamo, and D. Muñoz de la Peña. Fault-tolerant model predictive control. In *IEEE Conference on Emerging Technologies and Factory Automation (ETFA'2010)*, pages 1–8, 2010.

[5] Matthew Ellis, Helen Durand, and Panagiotis D. Christofides. A tutorial review of economic model predictive control methods. *Journal of Process Control*, 24(8):1156 – 1178, 2014.

[6] I. B. Gertsbakh. *Reliability Theory with Application to Preventive Maintenance*. Springer-Verlag, 2000.

[7] F. Guenab, P. Weber, D. Theilliol, and Y. M. Zhang. Design of a fault tolerant control system incorporating reliability analysis and dynamic behaviour constraints. *International Journal of Systems Science*, 42(1):219–233, 2011.

[8] D. Limon, M. Pereira, D. Muñoz de la Peña, T. Alamo, and J.M. Grosso. Single-layer economic model predictive control for periodic operation. *Journal of Process Control*, 8(24):1207–1224, August 2014.

[9] J.M. Maciejowski. *Predictive Control with Constraints*. Prentice Hall, Great Britain, 2002.

[10] Ministry of Work and Social Affairs. Ntp 417: Quantitative risk analysis - reliability of components and implications in preventive maintenance (in spanish only). Technical report, Spain, 2008.

[11] H. Noura, D. Theilliol, J.C. Ponsart, and A. Chamssedine. *Fault tolerant control systems: Design and practical application*. Springer Verlag, 2009.

[12] C. Ocampo-Martinez and V. Puig. Fault-tolerant model predictive control in the hybrid systems framework: Application to sewer networks. *International Journal of Adaptive Control and Signal Processing*, 23(8):757–787, 2009.

[13] C. Ocampo-Martinez, V. Puig, G. Cembrano, and J. Quevedo. Application of predictive control strategies to the management of complex networks in the urban water cycle. *Control Systems, IEEE*, 33(1):15–41, 2013.

[14] A. Ostfeld. Reliability analysis of regional water distribution systems. *Urban Water*, 3:253–260, 2001.

[15] J. Pascual, J. Romera, V. Puig, G. Cembrano, R. Creus, and M. Minoves. Operational predictive optimal control of Barcelona water transport network. *Control Engineering Practice*, 21(8):1020–1034, 2013.

[16] I. Prodan, E. Zico, and F. Stoican. Fault tolerant predictive control design for reliable microgrid energy management under uncertainties. *Energy*, 91:20 – 34, 2015.

[17] D. M. Raimondo, G. R. Marseglia, R. Braatz, and J. K. Scott. Fault-tolerant model predictive control with active fault isolation. In *2nd Conference on Control and Fault-Tolerant Systems (SysTol)*, pages 444–449, Nice, France, 2013.

[18] J. B. Rawlings, D. Angeli, and C. N. Bates. Fundamentals of economic model predictive control. In *51st IEEE Conference on Decision and Control*, Maui, Hawaii, USA, 2012.

[19] D. Robles, V. Puig, C. Ocampo-Martinez, and L. E. Garza. Methodology for actuator fault tolerance evaluation of linear constrained MPC: Application to the Barcelona water network. In *20th Mediterranean Conference on Control Automation (MED)*, pages 518–523, july 2012.

[20] J. Salazar, P. Weber, R. Sarrate, D. Theilliol, and F. Nejari. MPC design based on a DBN reliability model: application to drinking water networks. In *9th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, pages 688–693, Paris, France, 2015.

[21] H. Sanchez, T. Escobet, V. Puig, and Odgaard P. F. Health-aware model predictive control of wind turbines using fatigue prognosis. In *9th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, pages 1363–1368, Paris, France, 2015.

[22] D.D. Šiljak. *Decentralized control of complex systems*. Academic Press, 1991.

[23] M. Staroswiecki and D. Berdjag. A general fault tolerant linear quadratic control strategy under actuator outages. *International Journal of Systems Science*, 41(8):971–985, 2010.

[24] M. Staroswiecki, C. Commault, and J.M. Dion. Fault tolerance evaluation based on the lattice of system configurations. *International Journal of Adaptive Control and Signal Processing*, 26:54–72, 2012.

[25] A. Torii and R. Lopez. Reliability analysis of water distribution networks using the adaptive response surface approach. *Journal of Hydraulic Engineering*, 138:227–236, 2012.

[26] Y. Wang, C. Ocampo-Martinez, and V. Puig. Robust model predictive control based on Gaussian processes: Application to drinking water networks. In *European Control Conference*, Linz (Austria), 2015.

[27] P. Weber, C. Simon, D. Theilliol, and V. Puig. Fault-tolerant control design for over-actuated system conditioned by reliability: A drinking water network application. In *8th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (Safeprocess12)*, Mexico City, Mexico, 2012.

[28] X. Yang and J. Maciejowski. Fault-tolerant model predictive control of a wind turbine benchmark. In *8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, pages 337–342, Mexico City, Mexico, 2012.

[29] A. Yetendje, M. Seron, and J. De Doná. Fault-tolerant model predictive control in the hybrid systems framework: Application to sewer networks. *International Journal of Applied Mathematics and Computer Science*, 22(1):211–223, 2012.

[30] Y. Zhang and J. Jiang. Bibliographical review on reconfigurable fault-tolerant control systems. *Annual Reviews in Control*, 32(2):229 – 252, 2008.