Diagnosis and Fault-Tolerant Control of Critical Infrastructures

Vicenç Puig[1,2(✉)]

[1] Institut de Robtica i Informtica Industrial (CSIC-UPC), Barcelona, Spain
vicenc.puig@upc.edu
[2] Research Center for Supervision,
Safety and Automatic Control (UPC), Terrassa, Spain

Abstract. In modern societies, the reliable and continuous operation of certain infrastructures plays a fundamental role in the quality of life, economic development and security of nations. This paper presents several approaches for diagnosis and fault-tolerant control of critical infrastructure systems (CIS) including: the analysis of these systems to understand the weaknesses and risks in case some fault occurs, fault diagnosis using analytical redundancy relation, fault tolerant control schemes and assessment of the fault tolerance and inclusion of health-aware mechanisms in the CIS control systems.

Keywords: Fault diagnosis · Fault tolerant control · Sensor validation and reconstruction · Critical infrastructure systems

1 Introduction

In modern societies, the reliable and continuous operation of certain infrastructures plays a fundamental role in the quality of life, economic development and security of nations. Large-scale critical infrastructure systems (CIS), especially those located in urban areas (as drinking water or gas/energy infrastructures), is a subject of increasing concern. Because of this, these infrastructures are considered critical being very important to develop management systems that guarantee a reliable and continuous operation of these infrastructures. Other important aspects of the management of these infrastructures is that their operation must use efficiently the resources that they deliver (e.g., water, gas, ...), and also be efficient from an economic point of view and guarantee future supply. The critical nature of these infrastructures makes necessary a management system able to take into account their specific features and operation limits in presence of the uncertainties related to their operation. Thus, it is of paramount importance to have a control system in the management system that, from sensor measurements and available predictions of external influential variables, finds the proper way to operate the infrastructure in an efficient, safe and continuous manner.

This paper presents several approaches for diagnosis and fault-tolerant control of CIS including:

J.M. Kościelny et al. (eds.), *Advanced Solutions in Diagnostics and Fault Tolerant Control*, Advances in Intelligent Systems and Computing 635,
DOI 10.1007/978-3-319-64474-5_1

- the analysis of these systems to understand the weaknesses and risks in case some fault appears;
- fault diagnosis based on analytical redundancy relations.
- fault tolerant control schemes and assessment of the fault tolerance.
- inclusion of health-aware mechanism in the CIS control system.

The structure of the paper is the following: In Sect. 2, the fault diagnosis and fault-tolerant control of CIS is presented. Section 3 describes the tools for analysis of these systems to understand the weaknesses and risks in case some fault appears. Section 4 addresses the fault diagnosis problem, while Sect. 5 describes how to deal with the fault-tolerant control problem. The reliability analysis is presented in Sect. 6 and its use in the development of a health-aware control is intrdouced in Sect. 7. Finally, the conclusions are presented in Sect. 8.

2 Problem Set-Up

2.1 Control and Diagnosis Oriented Model

This paper considers a general CIS represented by a digraph $G(\mathcal{V}, \mathcal{E})$ (see [17] 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 CIS function, matter/energy is transported along the links by n_u flow actuators (e.g.., pipes and valves), passing through storage elements (as e.g., reservoirs or tanks), from specific origin locations to specific destination locations. The CIS is subject to several capacity and operational constraints, and to measured stochastic flows to customer sinks as driven by demand.

Selecting the storage level 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 CIS may be described by the following set of linear (or linearized) discrete-time difference-algebraic equations (DAE) for all time instants $k \in \mathbb{Z}_+$:

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

$$0 = \mathbf{E}_u\mathbf{u}(k) + \mathbf{E}_d\mathbf{d}(k), \tag{1b}$$

where the difference equation in (1a) describes the dynamics of the storage elements, and the algebraic equation in (1b) describes static relations in the CIS (i.e., mass/energy balance at junction nodes). Moreover, $\mathbf{A}, \mathbf{B}, \mathbf{B}_d, \mathbf{E}_u$ and $\mathbf{E}_d$ are time-invariant matrices of suitable dimensions as dictated by the CIS topology.

System (4) is subject to hard state and input polytopic constraints given by:

$$\mathcal{U} \triangleq \left\{\mathbf{u} \in \mathbb{R}^{n_u} \,|\, \mathbf{u}^{\min} \leq \mathbf{u} \leq \mathbf{u}^{\max}\right\}, \tag{2a}$$

$$\mathcal{X} \triangleq \left\{\mathbf{x} \in \mathbb{R}^{n_x} \,|\, \mathbf{x}^{\min} \leq \mathbf{x} \leq \mathbf{x}^{\max}\right\}, \tag{2b}$$

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

2.2 Statement of the Control Problem

Usually, the CIS modelled as in (4) is controlled using an MPC law that aims to minimize the operational costs as proposed in economic model predictive control (EMPC) [5,8,16]. 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

$$\mathbb{O}: \qquad \min_{\tilde{\mathbf{x}}, \tilde{\mathbf{u}}} J(\tilde{\mathbf{x}}, \tilde{\mathbf{u}}), \tag{3a}$$

subject to:

$$\mathbb{C}: \tag{3b}$$
$$\mathbf{x}(k+i+1|k) = \mathbf{A}\mathbf{x}(k+i|k) + \mathbf{B}\mathbf{u}(k+i|k) + \mathbf{B}_d\mathbf{d}(k+i|k), \forall i \in \mathbb{Z}_{[0,H_p-1]} \tag{3c}$$
$$\mathbf{0} = \mathbf{E}_u\mathbf{u}(k+i|k) + \mathbf{E}_d\mathbf{d}(k+i|k), \quad \forall i \in \mathbb{Z}_{[0,H_p-1]}, \tag{3d}$$
$$\mathbf{u}(k+i|k) \in \mathcal{U}, \quad \forall i \in \mathbb{Z}_{[0,H_p-1]}, \tag{3e}$$
$$\mathbf{x}(k+i|k) \in \mathcal{X}, \quad \forall i \in \mathbb{Z}_{[1,H_p]}, \tag{3f}$$

where

$$\tilde{\mathbf{x}} = (\mathbf{x}(1|k), \ldots, \mathbf{x}(N|k)), \tag{4a}$$
$$\tilde{\mathbf{u}} = (\mathbf{u}(0|k), \mathbf{u}(1|k), \ldots, \mathbf{u}(N-1|k)), \tag{4b}$$
$$\tilde{\mathbf{d}} = (\mathbf{d}(0|k), \mathbf{d}(1|k), \ldots, \mathbf{d}(N-1|k)) \tag{4c}$$

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 [12,19] for more details).

The MPC law belongs to the set $\mathcal{U}$ and is obtained using the *receding horizon philosophy* [9,16]. This technique consists of solving the optimization problem (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 (3a)) is applied to the system. At time $k+1$, in order to compute $\mathbf{u}^*(0|k+1)$ the optimization problem (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 (3a) collects all the control objectives of the closed-loop system, taking the name *multiobjective cost function*. In general form, (3a) can be written as:

$$J(\tilde{\mathbf{x}}, \tilde{\mathbf{u}}) = \sum_{i=0}^{n_J} \sum_{k=0}^{N} J_i(k), \tag{5}$$

where n_J is the number of objectives and $J_{i,k}$ corresponds to the evaluation of each particular objective i at time k. For example, in the case of drinking water networks the objective function takes into account the water production/transportation costs, the safety of the supply and the smoothness of the actuators operation to preserve their life [10]

3 System Analysis

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

After the fault occurrence:

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

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 Sect. 5.1, the algorithms evaluate whether or not a given system property, denoted by $P(K)$, is satisfied [1]. Thus,

$$P_K = \begin{cases} 1 \text{ if the property is satisfied,} \\ 0 \text{ if the property is not satisfied.} \end{cases} \tag{6}$$

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

$$2^{I+} = \{K \subseteq I; P_K = 1\}, \tag{7}$$

$$2^{I-} = \{K \subset I; P_K = 0\}. \tag{8}$$

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:

- *Critical actuators*, i.e., the set of actuators that are required to satisfy P_K. For every analysis, 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:

- 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, 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 (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 Sect. 5.1). 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, 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).

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.

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[1]. 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[2] $G(\mathcal{V}, \mathcal{E})$ 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 1 and 2, Algorithm 1 will perform the structural controllability analysis for a given AFC.

Algorithm 1. Controllability analysis using the structural approach

1: Obtain the digraph $G = (\mathcal{V}, \mathcal{E})$ of the system model used for designing the MPC (related to the optimization problem in (3a)) given a particular AFC
2: From the system digraph $G = (\mathcal{V}, \mathcal{E})$, find the reachability matrix Γ
3: **for** each $\mathbf{x}_i \in \mathbb{R}^{n_x}, i = 1, ..., n_x$ **do**
4: **if** $\nexists \mathbf{u}_j \in \mathbb{R}^{n_u}, j = 1, ..., n_u \mid \Gamma_{ij} = 1$ **then**
5: AFC is *non input-reachable*
6: **else**
7: **if** *s-rank*$([\mathbf{A}\ \mathbf{B}]) \neq n$ **then**
8: is *non-structurally controllable*
9: **else**
10: is *structurally controllable*
11: **end if**
12: **end if**
13: **end for**

[1] See [1] for important definitions related to the topic.
[2] See [17] for details on how to obtain a digraph from the system model.

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 (2) are considered, it is not possible to use the structural analysis algorithm[3]. presented in Sect. 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 (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)[4] can be checked using Algorithm 2.

Algorithm 2. Feasibility analysis

1: **for** $k = 1$ to H_p **do**
2: $\quad \mathcal{U}(k-1) \Leftarrow \mathcal{U}$
3: $\quad \mathcal{X}(k) \Leftarrow \mathcal{X}$
4: **end for**
5: $\mathcal{W} \Leftarrow \{\overbrace{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{H_p}}^{\bar{\mathbf{x}}}, \overbrace{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{H_p-1}}^{\bar{\mathbf{u}}}\}$
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: $\quad$ AFC is *admissible*
11: **else**
12: $\quad$ AFC is *non-admissible*
13: **end if**

Performance Analysis Algorithm The degradation of the control objective in a faulty situation can be quantified by means of maximal loss of efficiency ρ with respect to the objective function in a non-faulty situation J_0. This fact establishes whether of not the control objective 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 2, modifying the constraints defined in step 7 to add a new constraint:

$$\phi_{x_{H_p}} + \sum_{i=0}^{H_p-1} \Phi_i(\mathbf{x}_i, \mathbf{u}_i) \leq (1+\rho)\, J_0. \tag{9}$$

[3] 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.

[4] In case that an accommodation strategy is used, the faulty model used in Algorithm 2 should be replaced by the one used in (16).

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[5] can be proved by Algorithm 2 but including the new constraint (9), which considers the admissibility condition with respect to control performance over the prediction horizon H_p stated in the MPC controller.

4 Fault Diagnosis

The design of fault diagnosis system for a CIS involves building a set of consistency relations that only involves observed variables [4], known as Analytical Redundancy Relations (ARRs). To obtain ARRs for state space representation such as, it is necessary to manipulate the model to eliminate the unobserved variables (i.e., the state $\mathbf{x}$).

Given the model defined in corresponding to a known operating mode with observed variables $\mathbf{y}$ and $\mathbf{u}$, an ARR is defined as follows:

$$\Psi_i(\mathbf{y}, \mathbf{u}) = 0, \tag{10}$$

where Ψ_i is called the residual generator or computational form of residual r_i. The set of residuals, $\mathcal{W}$, can be represented as

$$\mathcal{W} = \{r_i | r_i = \Psi_i(\mathbf{y}, \mathbf{u}), i = 1, \ldots, n_r\}, \tag{11}$$

where n_r is the number of residuals.

Then, fault diagnosis is based on monitoring the set of residuals in order to assess the consistency of their corresponding ARRs. The set of inconsistent ARRs is represented by the set of residuals

$$\mathcal{W}^* = \{r_i | r_i = \Psi_i(\mathbf{y}, \mathbf{u}) \neq 0, i = 1, \ldots, n_r\} \subseteq \mathcal{W}. \tag{12}$$

Fault isolation task starts by obtaining the observed fault signature, where each single fault signal indicator ϕ_i is defined as follows:

$$\phi_i = \begin{cases} 0 & \text{if} r_i \notin \mathcal{W}^*, \\ 1 & \text{if} r_i \in \mathcal{W}^*. \end{cases} \tag{13}$$

Typically the interface between fault detection and fault isolation is through a binary codification of the evaluation of every residual; this binary interface could lead to a wrong diagnosis when the residuals present different sensitivities and order/time of activation after the fault appearance [3], and also produce undesirable decision instability (chattering) due to the effect of the noise and uncertainties. In the literature, there are different approaches to deal with this problem. For example, [15] proposed an improved fault diagnosis approach based

[5] If an accommodation strategy is used, the fault model used in Algorithm 2 should be replaced by the one used in (16).

on the fuzzy evaluation of the residuals that considers not only binary information but also signs/sensitivities as well as the persistence of residual activation. Finally, in [14], the use of the Kramer function [13] is proposed for evaluating the residuals gradient and to compute a fault diagnosis signal.

Fault isolation is based on comparing the history of the fault diagnosis signals with some stored fault patterns based on an extension of the fault signature matrix (with includes other signal properties such as signs, occurrence order and time) and to use a decision logic algorithm for proposing the most probable fault candidate.

5 Fault-Tolerant Control

5.1 Inclusion of Fault-Tolerant Capabilities

The control problem $\langle \mathbb{O}, \mathbb{C}, \mathbb{U} \rangle$ described in Sect. 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 Θ_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 (4) used by the MPC controller is modified as follows:

$$\mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k) + \sum_{i \in I_N} \mathbf{B}_i \mathbf{u}(k,i) + \mathbf{B}_d \mathbf{d}(k), \tag{14}$$

$$\mathbf{0} = \sum_{i \in I_N} \mathbf{E}_{u,i} \mathbf{u}(k,i) + \mathbf{E}_d \mathbf{d}(k), \tag{15}$$

   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 (4) used by the MPC controller should be modified as follows:

$$\mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k) + \sum_{i \in I_N} \mathbf{B}_i \mathbf{u}(k,i) + \sum_{i \in I_F} \beta_i(\mathbf{u}(k,i), \theta_i) + \mathbf{B}_d \mathbf{d}(k), \tag{16}$$

$$\mathbf{0} = \sum_{i \in I_N} \mathbf{E}_{u,i} \mathbf{u}(k,i) + \sum_{i \in I_F} \varepsilon_i(\mathbf{u}(k,i), \theta_i) + \mathbf{E}_d \mathbf{d}(k), \tag{17}$$

   where the functions β_i and ε_i and the parameters θ_i should be estimated by the FDI module for actuators belonging to the faulty actuator subset I_F.

Note that, in changing the model (4) 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.

6 Reliability Analysis

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 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 CIS, reliability is understood as its ability to provide an efficient matter/energy supply to consumers under both normal and abnormal operating conditions. For this reason, reliability is a measure of CIS performance. Reliability in CIS has already been considered in the literature [11,18].

When a reconfiguration FTC strategy is used, the reliability of CIS 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 CIS 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:

$$R_p(k) = 1 - \prod_{i=1}^{n_p} (1 - R_i(k)). \tag{18}$$

– Reliability of n_s serial subsystems is defined as:

$$R_s(k) = \prod_{i=1}^{n_s} R_i(k), \tag{19}$$

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

$$R_i(k) = e^{-k\gamma_i(k)}. \tag{20}$$

Thus, overall system reliability is given by

$$R_g(k) = \prod_{i=1}^{n_s}(1 - \prod_{i=1}^{n_p}(1 - R_i(k))). \tag{21}$$

Algorithm 3 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:

	p_1	p_2	p_3	$\ldots$	$p_{n_{ph}}$
u_1	1	0	1	$\ldots$	0
u_2	0	1	1	$\ldots$	1
u_3	1	0	0	$\ldots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
u_{n_u}	0	1	1	$\ldots$	1

(22)

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.

Algorithm 3. Reliability analysis

1: Decompose the system in n_p parallel subsystems and n_s subsystems using the system graph.
2: **for** $i = 1$ to n_u **do**
3: Evaluate actuator reliability $R_i(k)$ using (20).
4: **end for**
5: **for** $g = 1$ to n_p **do**
6: Evaluate reliability of parallel subsystems $R_{p,k}$ using (18) and (20).
7: **end for**
8: **for** $g = 1$ to n_s **do**
9: Evaluate reliability of system $R_g(k)$ using (21) and the result obtained from the evaluation in (20).
10: **end for**

7 Health-Aware Control

When a fault occurs, the MPC law is modified to cope with the fault, as discussed in Sect. 5.1. 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:

$$\gamma_i(k) = \gamma_i^o e^{\beta_i \mathbf{u}_i(k)}, \tag{23}$$

where γ_i^o represents the baseline failure rate (nominal failure rate) and $\mathbf{u}_i$ is the control action for the i-*th* actuator. Parameter β_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:

$$R_i(k) = e^{k\gamma_i} = e^{\gamma_i^o e^{k\beta_i \mathbf{u}_i(k)}}. \tag{24}$$

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 (24) as follows:

$$|u_{i,th}| = \frac{1}{\beta_i} \ln\left(\frac{\ln R_{i,th}}{\gamma_i^o k_{end}}\right). \tag{25}$$

Hence, the MPC controller (3a) can be redesigned by including the following constraint in the i-*th* actuator control:

$$u_i \in [-u_{i,th}, u_{i,th}]. \tag{26}$$

However, as discussed in [20], this will only preserve the reliability of the i-*th* actuator. In order to preserve the reliability of the whole CIS, the new actuator constraints (26) should be derived taking into account the reliability expression (19) 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 4, which considers, as constraints, the reliability of the cis in (19) derived by means of Algorithm 3 in terms of the reliability of each actuator, the impact of actuator load (see (24)) and the actuator operational constraints defined in (3a).

After solving the CSP problem in Algorithm 4, to solve the optimization problem associated the MPC design, the resulting updated actuator constraints

Algorithm 4. Health-aware MPC

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

are used instead of the actuator operational constraints defined in (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 CIS performance but will extend the life of the remaining actuators.

8 Conclusions

This paper has presented several approaches for diagnosis and fault-tolerant control of critical infrastructure systems (CIS) including: the analysis of these systems to understand the weaknesses and risks in case some fault occurs, fault diagnosis using analytical redundancy relation, fault tolerant control schemes and assessment of the fault tolerance and inclusion of health-aware mechanisms in the CIS control systems. The proposed approach combines structural, feasibility, performance and reliability analyses. After a fault, the CIS 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.

References

1. Blanke, M., Kinnaert, M., Lunze, J., Staroswiecki, M.: Diagnosis and Fault-Tolerant Control, 3rd edn. Springer-Verlag, Berlin, Heidelberg (2016)

2. Bondy, J., Murty, U.: Graph Theory with Applications. MacMillan Press, Great Britain (1982)
3. Combastel, C., Gentil, S., Rognon, J.P.: Toward a better integration of residual generation and diagnostic decision. In: 5^{th} IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes. Washington (2003)
4. Cordier, M.O., Dague, P., Lvy, F., Montmain, J., Staroswiecki, M., Trav–Massuys, L.: Conflicts versus analytical redundancy relations: a comparative analysis of the model based diagnosis approach from the artificial intelligence and automatic control perspectives. IEEE Trans. Syst., Man, Cybern. B **34**(5), 2163–2177 (2004)
5. Ellis, M., Durand, H., Christofides, P.D.: A tutorial review of economic model predictive control methods. J. Process Control **24**(8), 1156–1178 (2014)
6. Gertsbakh, I.B.: Reliability Theory with Application to Preventive Maintenance. Springer, Berlin (2000)
7. Guenab, F., Weber, P., Theilliol, D., Zhang, Y.M.: Design of a fault tolerant control system incorporating reliability analysis and dynamic behaviour constraints. Int. J. Syst. Sci. **42**(1), 219–233 (2011)
8. Limon, D., Pereira, M., Muñoz de la Peña, D., Alamo, T., Grosso, J.: Single-layer economic model predictive control for periodic operation. J. Process Control **8**(24), 1207–1224 (2014)
9. Maciejowski, J.: Predictive Control with Constraints. Prentice Hall, Great Britain (2002)
10. Ocampo-Martinez, C., Puig, V., Cembrano, G., Quevedo, J.: Application of predictive control strategies to the management of complex networks in the urban water cycle. Control Syst. IEEE **33**(1), 15–41 (2013)
11. Ostfeld, A.: Reliability analysis of regional water distribution systems. Urban Water **3**, 253–260 (2001)
12. Pascual, J., Romera, J., Puig, V., Cembrano, G., Creus, R., Minoves, M.: Operational predictive optimal control of Barcelona water transport network. Control Eng. Pract. **21**(8), 1020–1034 (2013)
13. Petti, T.F., Klein, J., Dhurjati, P.S.: Diagnostic model processor: using deep knowledge for process fault diagnosis. AIChE J. **36**(4), 565–575 (1990)
14. Puig, V., Schmid, F., Quevedo, J., Pulido, B.: A new fault diagnosis algorithm that improves the integration of fault detection and isolation. In: 44^{th} IEEE Conference on Decision and Control and European Control Conference, pp. 3809–3814. Sevilla, Spain (2005)
15. Ragot, J., Maquin, D.: Fault measurement detection in an urban water supply network. J. Process Control **16**(9), 887–902 (2006)
16. Rawlings, J.B., Angeli, D., Bates, C.N.: Fundamentals of economic model predictive control. In: 51st IEEE Conference on Decision and Control. Maui, Hawaii (2012)
17. Šiljak, D.: Decentralized control of complex systems. Academic Press, Boston (1991)
18. Torii, A., Lopez, R.: Reliability analysis of water distribution networks using the adaptive response surface approach. J. Hydraul. Eng. **138**, 227–236 (2012)
19. Wang, Y., Ocampo-Martinez, C., Puig, V.: Robust model predictive control based on Gaussian processes: application to drinking water networks. In: European Control Conference. Linz, Austria (2015)
20. Weber, P., Simon, C., Theilliol, D., Puig, V.: 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)