Supervisor Control of a Cyber-Physical Water Distribution Network in the Presence of Actuator and Sensor Faults

Dimitrios G. Fragkoulis[1[0000-0002-0177-5110]], Fotis N. Koumboulis[1[0000-0002-9856-049X]], Maria P. Tzamtzi[1[0009-0008-8930-1024]], and Nikolaos D. Kouvakas[1[0000-0001-5126-5226]]

[1]Robotics, Automatic Control and Cyber-Physical Systems Laboratory, Department of Digital Industry Technologies, School of Science, National and Kapodistrian University of Athens, Euripus Campus, 34400 Euboea, Greece.

Abstract. The models of the actuators (pumps, and valves) and water level sensors of a Water Distribution Network (WDN) testbed are presented, in the presence and the absence of faults, using Discrete Event System (DES) models in the Ramadge-Wonham framework. The cases of faults in the vertical valves, the pumps and the sensors are considered. In both the presence and the absence of faults, the desired behavior of the system is imposed in the form of rules with a parametric number of actuators and sensors. A hybrid supervisor control architecture will be designed based on the desired rules. The properties of the parametric controlled system are proved.

Keywords: Discrete Event Systems, Supervisor Control Theory, Water Distribution Networks.

1 Introduction

The coordination of the large number of interconnected devices installed in a Cyber-Physical System (CPS) is a challenge to be addressed by control system design (see [1]-[3]). Discrete Event Systems (DES) and Supervisor Control Theory (SCT) (see [4]-[7]) provide the background for the development of efficient coordinating tools for CPS ([8], [9]]). Moreover, the enhanced computational capabilities of modern control devices, such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs) and Supervisory Control And Data Acquisition (SCADA) systems facilitate the implementation of supervisor algorithms by drastically reducing the execution time and computational effort (see [10]-[13]).

Water Distribution Networks (WDNs) play a fundamental role in sustaining modern life, particularly when they provide clean and safe water for residential, commercial, and industrial use ([14]-[16]). These networks include reservoirs, pumping stations, treatment facilities, and pipelines, all of which rely on automated control systems to ensure efficient operation (see [14]-[16]).

In the present paper, a WDN testbed is studied. The testbed's detailed description can be found in [17]. An advantage of this testbed is the modularity of its components, covering various WDNs architectures and functionalities (see [18]-[21]). The DES models of the devices (actuators and sensors) of the testbed will be expressed parametrically. The analytic DES models of sensors and vertical actuators have first been presented in [22]. The analytic DES models of the horizontal valves will also be presented. The desired performance of the testbed will be expressed in the form of three rules referring to all actuators and sensors. The first two rules, referring to pumps and vertical valves, are the equivalent expressions, in "disable event form", of two rules in [22]. The present expression appears to be simpler and more adequate for their realization in supervisor form. The rules will be translated to a set of regular languages, being parametric with respect to the number of devices of the tank. Each regular language will be realized by a two-state finite deterministic supervisor automaton. The third rule, referring to horizontal valves, is expressed here for the first time. The third rule is in disjunctive form. Thus, it is proposed to be realized by a supervisor, being the disjunctive architecture of two supervisors. Regarding disjunctive architecture, see [5], [32] and [33]. Since the supervisors of the first two rules are designed in a conjunctive architecture (synchronous product [4]) and the supervisors of the third rule use a disjunctive architecture, the present design scheme constitutes a hybrid [4] architecture. The nonblocking property of the resulting controlled testbed ([4], [5], [23]) and the Physical Realizability (PR) ([24]) of the developed supervisor scheme will be proved. This is the first contribution of the present paper.

Next, in the present paper, the case of the presence of actuator and sensor faults will be studied by developing supervisors that will satisfy desired operation in the presence of faults. The cases of faults in the vertical valves, the pumps and the sensors will be studied. In this case of faults, nonblocking and PR will also be proved. This is the second contribution of the paper.

It is important to mention that in [22], the control of the testbed has been studied, without taking into account the horizontal valves of the testbed and without taking into consideration possible actuator and sensor faults. The contribution of the present work as compared to [22] is the development of the DES models in the presence of faults, the supervisor design using the horizontal valves and the design of resilient supervisors with respect to faults.

In Section 2, that follows, the testbed will be presented. In Section 3, the DES models of all pumps, valves, and water level sensors, will be presented. In Section 4, the DES models of the actuators and sensors will be developed in the presence of faults. In Section 5, the desired performance is presented in the form of rules and regular languages, and a set of supervisors will be developed realizing the desired languages. In Section 6, the desired performance in the presence of faults is presented in the form of rules and a set of supervisors will be developed.

2 Description of the Testbed

The HYDRA testbed is developed at the Modeling for Critical Infrastructures Protection (MCIP) Laboratory of Roma Tre University in Italy. The testbed represents a versatile platform for analyzing the behavior of WDNs [17]–[21]. It features a modular cyber-physical architecture that emulates many real-world WDNs. Both the cyber and physical components of the testbed are highly modular, enabling users to dynamically reconfigure system layouts and switch between different operational scenarios. This modularity of HYDRA is a key advantage that facilitates experimentation with a wide range of types of water networks, including networks for small cities and industrial cooling systems.

According to [17]–[21], the testbed comprises seven vertically arranged water tanks, as illustrated in Figure 1.

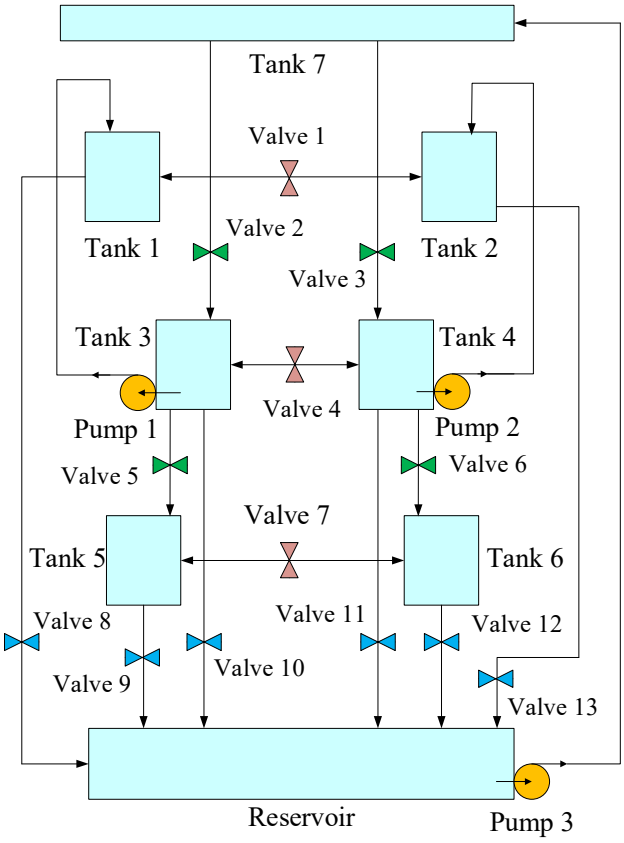

Fig. 1. Tanks, valves and pumps of the Hydra testbed

At the top of the setup, there is a large tank simulating a typical water tower, a common feature in urban water networks. Below there are six additional tanks distributed

across three distinct levels. Each tank is equipped with two types of sensors: an ultrasonic sensor, mounted at the top for non-contact water level measurement, and a submerged pressure sensor for continuous real-time monitoring. At the base of the configuration, there lies a reservoir, symbolizing an aquifer, which serves as the main water source for the network. These tanks are interconnected through non-pressurized piping, allowing gravity-driven water flow aided by pump action, in accordance with Stevin's Law. This design enables the recreation of numerous hydraulic and operational scenarios ([17]-[21]).

Water circulation within the system is facilitated by three pumps, as shown in Figure 1. The first pump draws water from the reservoir to the elevated water tower, while the remaining two pumps manage water transfer from the second to the third level. Each pump is independently controllable, allowing flexible system behavior simulation. To represent real-world water consumption, the system incorporates ten electromechanical valves, where the green colored valves represent the consumption ending in the tank of a lower level, while the blue colored valves represent the consumptions (or even leakage) ending in the reservoir (see Figure 1). These valves can be individually actuated to replicate diverse demand patterns. Additionally, three auxiliary valves (red in Figure 1) enable inter-tank connections, further enhancing the platform's adaptability and allowing the study of various flow dynamics and circulation scenarios.

The last tank of Hydra testbed, namely Tank 7, represents water source. Also, Pump 3 is used only to preserve continuous waterflow in the network. The part of Hydra that will be used here to represent a small scale WDN is the one that includes: Valve 1 to Valve 13, Pump 1 and Pump 2, as well as Tank 1 to Tank 6. In order to generalize the present WDN configuration, the total number of tanks is denoted as n_L, the total number of pumps is denoted as n_P, and the total number of valves is denoted as n_V. Since there is a single water level sensor installed in each tank, the number of water level sensors is n_L. So, the index $k \in \{1,...,n_L\}$ denotes the index of each tank and each level sensor. Regarding the Hydra testbed it holds that $n_L = 6$, $n_P = 2$, and $n_V = 13$. From Figure 1, it is observed that each tank indexed by an odd tank number is connected through a horizontal valve with one and only one tank, indexed by an even tank number, and vice versa. In the generalization of Hydra testbed, it is observed that the present pairwise configuration of tanks requires that the number of tanks under study, i.e., the number n_L, is an even number. Hence, the tanks can be grouped into pairs, where each pair is indexed by $\rho \in \{1,...,,n_L/2\}$, where

$$\rho = \begin{cases} (k+1)/2, & \text{if } k \text{ is odd} \\ k/2 & \text{if } k \text{ is even} \end{cases}. \quad (1)$$

Using this index, the pairs of tanks are in the form $(2\rho-1, 2\rho)$. For example, the pair of tanks of Hydra testbed that correspond to $\rho = 1$ is $(1,2)$. The pair that corresponds to $\rho = 2$ is $(3,4)$, and the pair that corresponds to $\rho = 3$ is $(5,6)$.

3 Modelling of the Devices of the Water Distribution Network without Faults

3.1 DES Models of the Actuators

The model of the actuators (see [22]) is:

$$\mathbf{G}_{i,j} = (\mathbb{Q}_{i,j}, \mathbb{E}_{i,j}, f_{i,j}, \mathbb{H}_{i,j}, x_{i,j,0}, \mathbb{Q}_{i,j,m}),\ i \in \{P,V\} \wedge j \in \{1,...,n_i\}$$

where index "*P*" corresponds to the model of the pumps and index "*V*" corresponds to the model of the valves. Also, n_i is the number of the respective devices installed in the network. Recall that n_P is the number of pumps and n_V is the number of valves. The state set of the actuator is $\mathbb{Q}_{i,j} = \{q_{i,j,1}, q_{i,j,2}\}$, where $q_{i,j,1}$ corresponds to the idle (non-working) mode of the device and $q_{i,j,2}$ corresponds to the working mode of the device. The initial state of the device is $x_{i,j,0} = q_{i,j,1}$. The marked state set of the device is $\mathbb{Q}_{i,j,m} = \{q_{i,j,1}\}$. The alphabet of the device is $\mathbb{E}_{i,j} = \{e_{i,j,1}, e_{i,j,2}\}$, where $e_{i,j,1}$ is the command to activate the device and $e_{i,j,2}$ is the command to deactivate the device. The active event sets of the device are $\mathbb{H}_{i,j}(q_{i,j,1}) = \{e_{i,j,1}\}$ and $\mathbb{H}_{i,j}(q_{i,j,2}) = \{e_{i,j,2}\}$. The transition function of the device is $f_{i,j}(q_{i,j,1}, e_{i,j,1}) = q_{i,j,2}$ and $f_{i,j}(q_{i,j,2}, e_{i,j,2}) = q_{i,j,1}$. The closed behavior [4] of $\mathbf{G}_{i,j}$ is $\mathbb{L}(\mathbf{G}_{i,j}) = \overline{(e_{i,j,1}e_{i,j,2})^*}$. Its marked behavior [4] is $\mathbb{L}_m(\mathbf{G}_{i,j}) = (e_{i,j,1}e_{i,j,2})^*$. The model $\mathbf{G}_{i,j}$ is nonblocking [11], i.e., $\mathbb{L}(\mathbf{G}_{i,j}) = \overline{\mathbb{L}_m(\mathbf{G}_{i,j})}$. The controllable event set ([4]-[5]) is $\mathbb{E}_{i,j,c} = \{e_{i,j,1}, e_{i,j,2}\}$ and the uncontrollable event set ([4]-[5]) is and $\mathbb{E}_{i,j,uc} = \varnothing$. The state diagram of the automaton $\mathbf{G}_{i,j}$ is depicted in Figure 2. The models of the actuators are in an input-output form (see [27]).

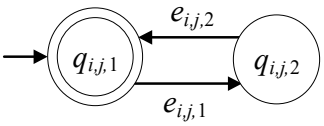

Fig. 2. State diagram of $\mathbf{G}_{i,j}$

3.2 Model of the Water Level Sensors

The model of the water level sensor is of the form [22]

$$\mathbf{G}_{L,k} = (\mathbb{Q}_{L,k}, \mathbb{E}_{L,k}, f_{L,k}, \mathbb{H}_{L,k}, x_{L,k,0}, \mathbb{Q}_{L,k,m}),\ k \in \{1,...,n_L\}.$$

The total number of water zones, measured by the k-th sensor being installed in the k-th tank, is denoted as m_k. The states' set is $\mathbb{Q}_{L,k} = \{q_{L,k,1},...,q_{L,k,m_k}\}$. Regarding the interpretation of the states, it holds that state $q_{L,k,\mu}$, $\mu \in \{1,...,m_k - 1\}$, corresponds to the μ-th zone's level, where the level of the water is between the lower limit and the upper limit of the zone. q_{L,k,m_k} corresponds to the state where the water level is higher

than the upper limit of the $m_k - 1$ zone. $x_{L,k,0} = q_{L,k,1}$ is the initial state. $\mathbb{Q}_{L,k,m} = \mathbb{Q}_{L,k}$ is the set of marked states. $\mathbb{E}_{L,k} = \{e_{L,k,1},...,e_{L,k,m_k-1}\}$ is the alphabet. $e_{L,k,\mu}$, $\mu \in \{1,...,m_k - 1\}$, is the event indicating that the water level is approaching the upper limit of the μ-th zone. The active event sets are

$$\mathbb{H}_{L,k}(q_{L,k,1}) = \{e_{L,k,1}\},\ \mathbb{H}_{L,k}(q_{L,k,\mu}) = \{e_{L,k,\mu}, e_{L,k,\mu-1}\};\ \mu \in \{2,...,m_k - 1\},$$
$$\mathbb{H}_{L,k}(q_{L,k,m_k}) = \{e_{L,k,m_k-1}\}.$$

The transition function is

$$f_{L,k}(q_{L,k,1}, e_{L,k,1}) = q_{L,k,2},\ f_{L,k}(q_{L,k,m_k}, e_{L,k,m_k-1}) = q_{L,k,m_k-1}$$
$$f_{L,k}(q_{L,k,\mu}, e_{L,k,\mu}) = q_{L,k,\mu+1},\ f_{L,k}(q_{L,k,\mu}, e_{L,k,\mu-1}) = q_{L,k,\mu-1};\ \mu \in \{2,...,m_k - 1\}.$$

The closed behavior of $\mathbf{G}_{L,k}$ is

$$\mathbb{L}(\mathbf{G}_{L,k}) = \overline{\left(e_{L,k,1}\left(e_{L,k,2}\cdots(e_{L,k,m_k-1}e_{L,k,m_k-1})^*\cdots e_{L,k,2}\right)^* e_{L,k,1}\right)^*}.$$

The marked behavior of $\mathbf{G}_{L,k}$ is $\mathbb{L}_m(\mathbf{G}_{L,k}) = \mathbb{L}(\mathbf{G}_{L,k})$. It is important to mention that all states of the automaton have been considered marked states, as all tank's level are accepted as "desired". Moreover, it is important to mention that in [22] only state $q_{L,k,1}$ was conventionally marked. In both cases the nonblocking proof is not affected as will proved in Sections 5 and 6. $\mathbf{G}_{L,k}$ is a nonblocking automaton. The controllable and uncontrollable events sets are $\mathbb{E}_{L,k,c} = \varnothing$, and $\mathbb{E}_{L,k,uc} = \mathbb{E}_{L,k}$, respectively. The state diagram of the automaton $\mathbf{G}_{L,k}$ is depicted in Figure 3.

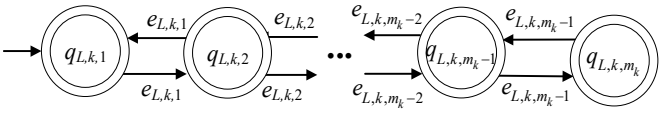

Fig. 3. State diagram of $\mathbf{G}_{L,k}$

4 Modelling of the Devices of the Water Distribution Network with Faults

4.1 Model of the Faults

The model of the fault of each device can be expressed as a two-state automaton of the form ([24]):

$$\mathbf{G}_{E,i,j} = (\mathbb{Q}_{E,i,j}, \mathbb{E}_{E,i,j}, f_{E,i,j}, \mathbb{H}_{E,i,j}, x_{E,i,j,0}, \mathbb{Q}_{E,i,j,m}),\ i \in \{P,V,L\} \wedge j \in \{1,...,n_i\}.$$

The set of states is $\mathbb{Q}_{E,i,j} = \{q_{E,i,j,1}, q_{E,i,j,2}\}$. Regarding the states' interpretation, it holds that state $q_{E,i,j,1}$ corresponds to the non-faulty case of the device, and state $q_{E,i,j,2}$ corresponds to the faulty case of the device. The alphabet is $\mathbb{E}_{E,i,j} = \{e_{E,i,j,1}, e_{E,i,j,2}\}$, where

$\mathbb{E}_{E,i,j,c} = \varnothing$ and $\mathbb{E}_{E,i,j,uc} = \mathbb{E}_{E,i,j}$. Regarding the events' interpretation, it holds that event $e_{E,i,j,1}$ corresponds to the signal that a fault has been detected, and event $e_{E,i,j,2}$ corresponds to the signal that the fault has been repaired. $x_{E,i,j,0} = q_{E,i,j,1}$ is the initial state and $\mathbb{Q}_{E,i,j,m} = \{q_{E,i,j,1}\}$ is the marked state set. Regarding the active events it holds that $\mathbb{H}_{E,i,j}(q_{E,i,j,1}) = \{e_{E,i,j,1}\}$, and $\mathbb{H}_{E,i,j}(q_{E,i,j,2}) = \{e_{E,i,j,2}\}$. The transition function is $f_{E,i,j}(q_{E,i,j,1}, e_{E,i,j,1}) = q_{E,i,j,2}$ and $f_{E,i,j}(q_{E,i,j,2}, e_{E,i,j,2}) = q_{E,i,j,1}$. It holds that $\mathbb{L}_m(\mathbf{G}_{E,i,j}) = (e_{E,i,j,1}e_{E,i,j,2})^*$, $\mathbb{L}(\mathbf{G}_{E,i,j}) = \overline{\mathbb{L}_m(\mathbf{G}_{E,i,j})}$.

4.2 The Models of the Devices in the presence of faults

The model of each device in the presence of faults can be calculated by using the corresponding model not including faults and the respective model of the fault of each device. Hence, the model of each device in the presence of faults is given by the automaton

$$\mathbf{G}_{F,i,j} = \mathbf{G}_{i,j} \,||\, \mathbf{G}_{E,i,j},\ i \in \{P,V,L\} \wedge j \in \{1,...,n_i\}$$

The set of the states is $\mathbb{Q}_{F,i,j} = \mathbb{Q}_{i,j} \times \mathbb{Q}_{E,i,j}$, the alphabet is $\mathbb{E}_{F,i,j} = \mathbb{E}_{i,j} \cup \mathbb{E}_{E,i,j}$, the initial state is $x_{F,i,j,0} = (q_{i,j,1}, q_{E,i,j,1})$ and the set of marked states is $\mathbb{Q}_{F,i,j,m} = \mathbb{Q}_{i,j,m} \times \{q_{E,i,j,1}\}$.

Remark 1: It is important to mention that an actuator fault results in the corresponding pump or valve to stuck in either the open or the closed position. On the other hand, a sensor fault provides unreliable information regarding the water level. Therefore, in both cases, whether a fault occurs either in an actuator or a sensor, appropriate control actions that are not based on faulty devices, must be developed.

Remark 2: In what follows, it is considered that a fault detection mechanism has been installed into the system to provide information for the detection of a fault and the determination of the respective faulty device (fault isolation). Regarding fault detection and isolation see [28]-[31]. Each fault detection event is distinct and non-repeatable, in the sense that it cannot be repeated unless the respective repair event has taken place. This is reflected in model $\mathbf{G}_{E,i,j}$, where between fault detection events the presence of a repair event is necessary.

5 Supervisor Design without faults

5.1 Behavior of the Water Distribution Network without Faults

The tanks of the WDN must preserve the desired water level. This means that the water level must be above a predefined zone and at the same time must not exceed the upper limit. Therefore, the actuators of the WDN, responsible for the rise and drop of the water level, must be controlled to guarantee the desired level. Let the pair (i, j), where $i \in \{P,V,L\}$, and $j \in \{1,...,n_i\}$. Recall that the first element of this pair denotes the type of device, i.e., pump, valve, and level sensor, and the second element denotes

the index of the device. Let $\mathbb{D}_k$ be the set containing all pairs of the forms (i, j), i.e., all the devices associated with the k-th tank. Obviously, the total number of devices associated with the k-th tank is $\ell_k = |\mathbb{D}_k|$, where $|\bullet|$ denotes the cardinality of the argument set. For instance, and according to Figure 1, Level sensor 1, Pump 1 and Valve 1 are associated with Tank 1, hence $\mathbb{D}_1 = \{(L,1),(P,1),(V,1)\}$, and $\ell_1 = |\mathbb{D}_1| = 3$. Let $\mathbb{D}_{I,k}$, $\mathbb{D}_{D,k}$ and $\mathbb{D}_{H,k}$ be subsets of $\mathbb{D}_k$. It holds that $\mathbb{D}_{I,k}$ contains all vertical actuator pairs of the k-th tank contributing to the water level increase, $\mathbb{D}_{D,k}$ contains all vertical actuator pairs of the k-th tank contributing to the water level decrease, and $\mathbb{D}_{H,k}$ contains the horizontal actuator pair of the k-th tank. According to Section 2, recall that ρ denotes the index of each pair of tanks, where $\rho \in \{1,...,n_L/2\}$. Obviously, it holds that $\mathbb{D}_{H,2\rho-1} = \mathbb{D}_{H,2\rho}$ and $\left|\mathbb{D}_{H,2\rho-1}\right| = 1$. From the above equalities it is observed that the pair of each horizontal valve can be expressed in the form

$$\left(V, \upsilon_H(\rho)\right) = (V, \xi) \in \mathbb{D}_{H,2\rho-1}; \rho \in \{1,...,n_L/2\}. \tag{2}$$

The rules describing the desired behavior of the actuators are the following:

Rule 1: If the k-th tank's level sensor has reached its maximum value, then the vertical actuators of $\mathbb{D}_{I,k}$, contributing to level increase, are not allowed to be activated.

Rule 2: If the k-th tank's level sensor has reached its minimum value, then the vertical actuators of $\mathbb{D}_{D,k}$, contributing to level decrease, are not allowed to be activated.

Rule 3: Only if the $2\rho-1$-th tank's level sensor or the 2ρ-th tank's level sensor, where $\rho \in \{1,...,n_L/2\}$ and is given in (1), has reached its minimum or maximum value, then the corresponding horizontal valve $\left(V, \upsilon_H(\rho)\right)$ is allowed to be activated.

The first two rules are the "disable event form" expressions of the respective rules in [22]. This "disable form" facilitates the expression of the corresponding regular languages in a more compact and simple form. The third rule, being introduced here for the first time, is in "enable event form" and is rather complex. The formal expression of this rule and its realization in supervisor form will be examined thoroughly.

The regular language formally expressing Rule 1, for the k-th tank, $k \in \{1,...,n_L\}$ and the vertical actuator $(\chi,\psi) \in \mathbb{D}_{I,k}$, is of the form

$$\mathbb{K}_{I,k}(\chi,\psi) = \overline{\left(e^*_{\chi,\psi,1} e_{L,k,m_k-1} e_{L,k,m_k-1}\right)^*}. \tag{3}$$

The regular language formally expressing Rule 2, for the k-th tank, $k \in \{1,...,n_L\}$ and the vertical actuator $(\chi,\psi) \in \mathbb{D}_{D,k}$, is of the form

$$\mathbb{K}_{D,k}(\chi,\psi)=\overline{\left(e_{L,k,1}e^{*}_{\chi,\psi,1}e_{L,k,1}\right)^{*}}. \quad (4)$$

The formal expression of Rule 3 as a regular language is extremely complex. To overcome this difficulty, Rule 3 is analyzed in four cases. In Case 1, the 2ρ-th tank's level is between its minimum and its maximum value. In Case 2, the 2ρ-th tank's level is below its minimum value or above its maximum value. In Case 3, the $2\rho-1$-th tank's level is between its minimum and its maximum value. In Case 4, the $2\rho-1$-th tank's level is below its minimum value or above its maximum value.

In Case 1, the desired behavior of the horizontal valve $\left(V,\upsilon_H(\rho)\right)$ is formally expressed by the regular language

$$^{1}\mathbb{K}_H(\rho)=\overline{\left(e^{*}_{V,\upsilon_H(\rho),1}(e_{L,2\rho-1,1}+e_{L,2\rho-1,m_{2\rho-1}-1})(e_{L,2\rho-1,1}+e_{L,2\rho-1,m_{2\rho-1}-1})\right)^{*}}. \quad (5)$$

In Case 2, the desired behavior of the horizontal valve $\left(V,\upsilon_H(\rho)\right)$ is formally expressed by the regular language $^{2}\mathbb{K}_H(\rho)=e^{*}_{V,\upsilon_H(\rho),1}$. In Case 3, the desired behavior of the horizontal valve $\left(V,\upsilon_H(\rho)\right)$ is formally expressed by the regular language

$$^{3}\mathbb{K}_H(\rho)=\overline{\left(e^{*}_{V,\upsilon_H(\rho),1}(e_{L,2\rho,1}+e_{L,2\rho,m_{2\rho}-1})(e_{L,2\rho,1}+e_{L,2\rho,m_{2\rho}-1})\right)^{*}}. \quad (6)$$

In Case 4, the desired behavior of the horizontal valve $\left(V,\upsilon_H(\rho)\right)$ is also formally expressed by the regular language $^{4}\mathbb{K}_H(\rho)=\,^{2}\mathbb{K}_H(\rho)=e^{*}_{V,\upsilon_H(\rho),1}$. The unification of the four cases, through an appropriate supervisor that will realize Rule 3, will be studied in Subsection 5.3.

5.2 Supervisors of the Water Distribution Network without Faults

The supervisor realizing $\mathbb{K}_{I,k}(\chi,\psi)$, where $k\in\{1,...,n_L\}$ and $(\chi,\psi)\in\mathbb{D}_{I,k}$, is denoted as $\mathbf{S}_{I,k}(\chi,\psi)$ and can be described as a two-state automaton, see Figure 4. The alphabet of the supervisor is $\mathbb{E}_{S,I,k}(\chi,\psi)=\{e_{\chi,\psi,1},e_{L,k,m_k-1}\}$. It holds that

$$\mathbb{H}_{S,I,k}(\chi,\psi)\left(q_{S,I,k,1}(\chi,\psi)\right)\cap\mathbb{E}_{S,I,k,uc}(\chi,\psi)=\mathbb{E}_{S,I,k,uc}(\chi,\psi),$$
$$\mathbb{H}_{S,I,k}(\chi,\psi)\left(q_{S,I,k,2}(\chi,\psi)\right)\cap\mathbb{E}_{S,I,k,uc}(\chi,\psi)=\mathbb{E}_{S,I,k,uc}(\chi,\psi)$$

and where $\mathbb{E}_{S,I,k,uc}(\chi,\psi)=\{e_{L,k,m_k-1}\}$ is the set of the uncontrollable events taking part in $\mathbf{S}_{I,k}(\chi,\psi)$. Hence, using the criterion in [24], it is observed that PR of the supervisor $\mathbf{S}_{I,k}(\chi,\psi)$ is guaranteed, as all uncontrollable events of $\mathbf{S}_{I,k}(\chi,\psi)$ are active to both of its states.

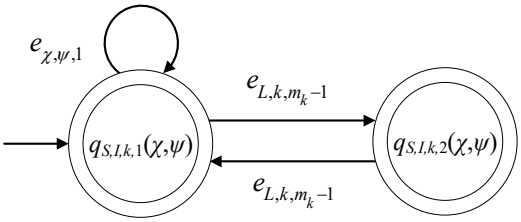

Fig. 4. State diagram of $\mathbf{S}_{I,k}(\chi,\psi)$.

The supervisor realizing $\mathbb{K}_{D,k}(\chi,\psi)$, where $k \in \{1,...,n_L\}$ and $(\chi,\psi) \in \mathbb{D}_{D,k}$, is denoted as $\mathbf{S}_{D,k}(\chi,\psi)$ and can be described also as a two-state automaton, see Figure 5. The alphabet of the supervisor is $\mathbb{E}_{S,D,k}(\chi,\psi) = \{e_{\chi,\psi,1}, e_{L,k,1}\}$. It holds that

$$\mathbb{H}_{S,D,k}(\chi,\psi)\left(q_{S,D,k,1}(\chi,\psi)\right) \cap \mathbb{E}_{S,D,k,uc}(\chi,\psi) = \mathbb{E}_{S,D,k,uc}(\chi,\psi),$$

$$\mathbb{H}_{S,D,k}(\chi,\psi)\left(q_{S,D,k,2}(\chi,\psi)\right) \cap \mathbb{E}_{S,D,k,uc}(\chi,\psi) = \mathbb{E}_{S,D,k,uc}(\chi,\psi)$$

and where $\mathbb{E}_{S,D,k,uc}(\chi,\psi) = \{e_{L,k,1}\}$ is the set of the uncontrollable events taking part in $\mathbf{S}_{D,k}(\chi,\psi)$. According to [24], PR of supervisor $\mathbf{S}_{D,k}(\chi,\psi)$ is also guaranteed.

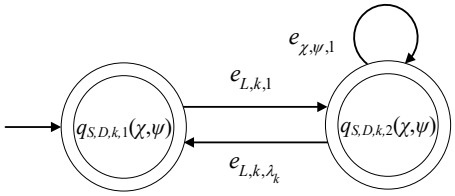

Fig. 5. State diagram of $\mathbf{S}_{D,k}(\chi,\psi)$.

The vertical actuators are restricted by the groups of supervisors denoted by $\mathbf{S}_{I,k}(\chi,\psi)$ and $\mathbf{S}_{D,k}(\chi,\psi)$. Activation of each vertical actuator may be enabled, according to Rules 1 and 2, provided that none of these supervisors restrict the corresponding activation event. This is accomplished by combining all supervisors $\mathbf{S}_{I,k}(\chi,\psi)$ and $\mathbf{S}_{D,k}(\chi,\psi)$ in a synchronous product architecture [4].

Regarding Rule 3, the respective supervisor architecture will be presented in the following two subsections. To this end, first, two supervisors will be developed. The first supervisor is denoted by ${}^1\mathbf{S}_H(\rho)$. This supervisor realizes the language ${}^1\mathbb{K}_H(\rho)$ and can be described as a two-state automaton, see Figure 6. The alphabet of the supervisor is ${}^1\mathbb{E}_{S,H}(\rho) = \{e_{V,\upsilon_H(\rho),1}, e_{L,2\rho-1,1}, e_{L,2\rho-1,m_{2\rho-1}-1}\}$. It holds that

$${}^1\mathbb{H}_{S,H}(\rho)\left({}^1q_{S,H,1}(\rho)\right) \cap {}^1\mathbb{E}_{S,H,uc}(\rho) = {}^1\mathbb{E}_{S,H,uc}(\rho),$$

$${}^1\mathbb{H}_{S,H}(\rho)\left({}^1q_{S,H,2}(\rho)\right) \cap {}^1\mathbb{E}_{S,H,uc}(\rho) = {}^1\mathbb{E}_{S,H,uc}(\rho)$$

and where ${}^{1}\mathbb{E}_{S,H,uc}(\rho) = \{e_{L,2\rho-1,1}, e_{L,2\rho-1,m_{2\rho-1}-1}\}$ is the set of uncontrollable events taking part in ${}^{1}\mathbf{S}_{H}(\rho)$. According to [24], PR of supervisor ${}^{1}\mathbf{S}_{H}(\rho)$ is also guaranteed.

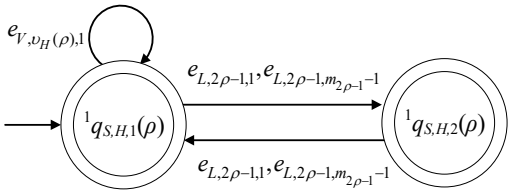

Fig. 6. State diagram of ${}^{1}\mathbf{S}_{H}(\rho)$.

The second supervisor is denoted by ${}^{3}\mathbf{S}_{H}(\rho)$. This supervisor realizes the language ${}^{3}\mathbb{K}_{H}(\rho)$ and can be described as a two-state automaton, see Figure 7. The alphabet of the supervisor is ${}^{3}\mathbb{E}_{S,H}(\rho) = \{e_{V,\upsilon_H(\rho),1}, e_{L,2\rho,1}, e_{L,2\rho,m_{2\rho}-1}\}$. It holds that

$$ {}^{3}\mathbb{H}_{S,H}(\rho)\left({}^{3}q_{S,H,1}(\rho)\right) \cap {}^{3}\mathbb{E}_{S,H,uc}(\rho) = {}^{3}\mathbb{E}_{S,H,uc}(\rho), $$

$$ {}^{3}\mathbb{H}_{S,H}(\rho)\left({}^{3}q_{S,H,2}(\rho)\right) \cap {}^{3}\mathbb{E}_{S,H,uc}(\rho) = {}^{3}\mathbb{E}_{S,H,uc}(\rho) $$

and where ${}^{3}\mathbb{E}_{S,H,uc}(\rho) = \{e_{L,2\rho,1}, e_{L,2\rho,m_{2\rho}-1}\}$ is the set of uncontrollable events taking part in ${}^{3}\mathbf{S}_{H}(\rho)$. According to [24], PR of supervisor ${}^{3}\mathbf{S}_{H}(\rho)$ is also guaranteed.

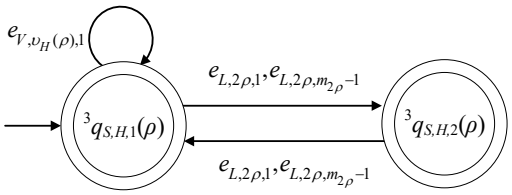

Fig. 7. State diagram of ${}^{3}\mathbf{S}_{H}(\rho)$.

5.3 Supervisor Design via Disjunctive Architecture for the Horizontal Valves of the WDN testbed without Faults

For each horizontal valve, Rule 3 permits the event that opens the valve to take place, if it is permitted by at least one of the formal specifications of the four cases. Using the model of the horizontal sensor (see the initial state), it is observed that for the satisfaction of Rule 3, it suffices to focus on the properties of the supervisors ${}^{1}\mathbf{S}_{H}(\rho)$ and ${}^{3}\mathbf{S}_{H}(\rho)$. Clearly, according to Rule 3, if at least one of these two supervisors permits the event that opens the valve to take place, then the event is permitted to take place. According to [5], [32], and [33], this requirement is expressed as a disjunctive architecture of the supervisors ${}^{1}\mathbf{S}_{H}(\rho)$ and ${}^{3}\mathbf{S}_{H}(\rho)$. Let the supervisor

$$\mathbf{S}_H(\rho) = {}^1\mathbf{S}_H(\rho) \llcorner\!\lrcorner {}^3\mathbf{S}_H(\rho)\,;\ \rho \in \{1,...,n_L/2\}\,. \tag{7}$$

where "$\llcorner\!\lrcorner$" is the symbol of the operator of disjunction between two automata. The operator of disjunction has similar properties to the synchronous product, except that a common event can trigger a transition, provided that it belongs to the active event set of the current state of either one of the two automata, see [5], [32] and [33]. The alphabet of $\mathbf{S}_H(\rho)$ is $\mathbb{E}_{S,H}(\rho) = {}^1\mathbb{E}_{S,H}(\rho) \cup {}^3\mathbb{E}_{S,H}(\rho)$, see also [5], [32] and [33].

5.4 Decentralized Architecture of the Controlled Water Distribution Network without Faults

Using compositional synthesis (see [7]), the automaton of the ρ-th pair of tanks is computed to be

$$\mathbf{G}(\rho) = \mathop{\|}_{(i,j)\in\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}} \mathbf{G}_{i,j}\,.$$

Note that "$\|$" is the symbol of the synchronous product [4] of two or more automata. The marked language of the automaton of the ρ-th pair of tanks is computed to be

$$\mathbb{L}_m(\mathbf{G}(\rho)) = \bigcap_{(i,j)\in\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}} P_{i,j}^{-1}\left(\mathbb{L}_m(\mathbf{G}_{i,j})\right),$$

where $P_{i,j}$ is the projection [6]-[7] of $\mathbb{E}_{i,j}^*$ to $\mathbb{E}^*(\rho)$ and $\mathbb{E}(\rho) = \bigcup_{(i,j)\in\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}} \mathbb{E}_{i,j}$. The controlled automaton of $\mathbf{G}(\rho)$ is determined to be

$$\mathbf{G}_c(\rho) = \mathbf{G}(\rho) \,\|\, \mathbf{S}_H(\rho) \,\|\left(\mathop{\|}_{\zeta\in\{I,D\}}\left(\left(\mathop{\|}_{(\chi,\psi)\in\mathbb{D}_{\zeta,2\rho-1}} \mathbf{S}_{\zeta,2\rho-1}(\chi,\psi)\right)\|\left(\mathop{\|}_{(\chi,\psi)\in\mathbb{D}_{\zeta,2\rho}} \mathbf{S}_{\zeta,2\rho}(\chi,\psi)\right)\right)\right),$$

$$\rho = 1,...,n_L/2\,.$$

The marked language of $\mathbf{G}_c(\rho)$ is

$$\mathbb{L}_m(\mathbf{G}_c(\rho)) = \mathbb{L}_m(\mathbf{G}(\rho)) \cap P_{H,\rho}^{-1}\left(\mathbb{L}_m(\mathbf{S}_H(\rho))\right) \cap$$

$$\bigcap_{\zeta\in\{I,D\}}\left(\left(\bigcap_{(\chi,\psi)\in\mathbb{D}_{\zeta,2\rho-1}}\left(P_{\zeta,2\rho-1}^{-1}(\chi,\psi)\left(\mathbb{K}_{\zeta,2\rho-1}(\chi,\psi)\right)\right)\right)\right) \cap$$

$$\bigcap_{\zeta\in\{I,D\}}\left(\left(\bigcap_{(\chi,\psi)\in\mathbb{D}_{\zeta,2\rho}}\left(P_{\zeta,2\rho}^{-1}(\chi,\psi)\left(\mathbb{K}_{\zeta,2\rho}(\chi,\psi)\right)\right)\right)\right)$$

where $P_{\zeta,2\rho-1}(\chi,\psi)$ is the projection of $\mathbb{E}_{S,\zeta,2\rho-1}^*(\chi,\psi)$ to $\mathbb{E}^*(\rho)$, $P_{\zeta,2\rho}(\chi,\psi)$ is the projection of $\mathbb{E}_{S,\zeta,2\rho}^*(\chi,\psi)$ to $\mathbb{E}^*(\rho)$ and $P_{H,\rho}$ is the projection of $\mathbb{E}_{S,H}^*(\rho)$ to $\mathbb{E}^*(\rho)$. It is noted that $\mathbb{E}_{S,\zeta,2\rho-1}(\chi,\psi)$ is the alphabet of the language $\mathbb{K}_{\zeta,2\rho-1}(\chi,\psi)$ and $\mathbb{E}_{S,\zeta,2\rho}(\chi,\psi)$ is the alphabet of the language $\mathbb{K}_{\zeta,2\rho}(\chi,\psi)$, where $\zeta \in \{I,D\}$.

The total controlled automaton of the WDN is

$$\tilde{\mathbf{G}}_c = \mathop{\|}_{\rho=1}^{n_L/2} \mathbf{G}_c(\rho)\,.$$

The marked language of $\tilde{\mathbf{G}}_c$ is

$$\mathbb{L}_m(\tilde{\mathbf{G}}_c) = \bigcap_{\rho=1}^{n_L/2} P_\rho^{-1}\left(\mathbb{L}_m(\mathbf{G}_c(\rho))\right),$$

where P_ρ is the projection of $\mathbb{E}^*(\rho)$ to $\mathbb{E}^*$, where $\mathbb{E}=\bigcup_{\rho=1}^{n_L/2}\mathbb{E}(\rho)$.

Remark 3: The nonblocking property of the controlled automaton is proved, as it holds that:

- The supervisors are PR with respect to the total automaton of the system.
- Only events, being responsible for the transition from the marked state to the non-marked state, are restricted by the supervisors.

6 Supervisor Design with Faults

6.1 Behavior of the Water Distribution Network with Faults

According to Remark 1, in case of actuator and/or sensor faults, then a different supervisor control strategy must be applied to the system. Hence, the supervisor design must be extended to face the presence of faults in vertical valves, in the two pumps involved in the water network and the sensors. To this end, it is proposed that the first two rules in Section 5 remain unchanged, and a new and extended version of the Rule 3 is developed as follows:

Rule 3: Only if either the water level sensor of $2\rho-1$-th or 2ρ-th tank has reached its minimum or maximum value, or a device of $2\rho-1$-th or 2ρ-th tank, except the $(V,\upsilon_H(\rho))$ valve, is in fault, then the corresponding horizontal valve $(V,\upsilon_H(\rho))$ is allowed to be activated.

The regular languages of Rules 1 and 2 have been presented in Section 5. As already mentioned in Section 5, the formal expression of Rule 3 is analyzed into four cases. Here, except for these four cases, additional cases are introduced. Each additional case is the case of the presence of faults in the corresponding device of the pair of tanks. Recall that $\mathbb{D}_{2\rho-1}$ contains all pairs that describe the devices associated with the $2\rho-1$-th tank. Also, recall that $\mathbb{D}_{2\rho}$ contains all pairs that describe the devices associated with the 2ρ-th tank. Recall that the presence of faults in the horizontal valves of the WDN testbed is out the scope of the present paper. Hence, the presence of faults in the devices described by the pairs $(\chi,\psi)\in\left(\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}\right)-\left\{(V,\upsilon_H(\rho))\right\}$ will be considered. The desired behavior of each additional case, is formally expressed by the language

$$^{(\chi,\psi)}\mathbb{K}_H(\rho) = \overline{\left(e^*_{E,\chi,\psi,2}e_{E,\chi,\psi,1}(e_{V,\upsilon_H(\rho),1}+e_{E,\chi,\psi,1})^* e_{E,\chi,\psi,2}\right)^*};$$
$$(\chi,\psi)\in\left(\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}\right)-\left\{(V,\upsilon_H(\rho))\right\} \quad (8)$$

The unification of all additional cases, through an appropriate supervisor that will realize Rule 3, will be studied in Subsection 6.2.

6.2 Resilient Supervisor of the Water Distribution Network

The supervisor of the language in (8) will be developed. The supervisor is denoted as ${}^{(\chi,\psi)}\mathbf{S}_H(\rho)$ and is expressed as a two-state automaton, see Figure 8. The alphabet of the supervisor is ${}^{(\chi,\psi)}\mathbb{E}_{S,H}(\rho)=\{e_{V,\upsilon_H(\rho),1},e_{E,\chi,\psi,1},e_{E,\chi,\psi,2}\}$. It holds that

$$ {}^{(\chi,\psi)}\mathbb{H}_{S,H}(\rho)\left({}^{(\chi,\psi)}q_{S,H,1}(\rho)\right)\cap {}^{(\chi,\psi)}\mathbb{E}_{S,H,uc}(\rho)={}^{(\chi,\psi)}\mathbb{E}_{S,H,uc}(\rho), $$
$$ {}^{(\chi,\psi)}\mathbb{H}_{S,H}(\rho)\left({}^{(\chi,\psi)}q_{S,H,2}(\rho)\right)\cap {}^{(\chi,\psi)}\mathbb{E}_{S,H,uc}(\rho)={}^{(\chi,\psi)}\mathbb{E}_{S,H,uc}(\rho) $$

and where ${}^{(\chi,\psi)}\mathbb{E}_{S,H,uc}(\rho)=\{e_{E,\chi,\psi,1},e_{E,\chi,\psi,2}\}$ is the set of uncontrollable events taking part in ${}^{(\chi,\psi)}\mathbf{S}_H(\rho)$. According to [24], PR of supervisor ${}^{(\chi,\psi)}\mathbf{S}_H(\rho)$ is also guaranteed.

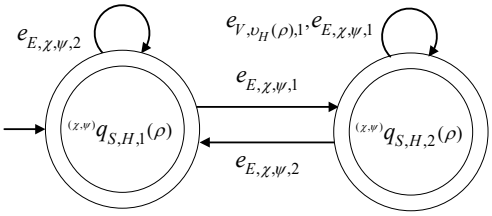

Fig. 8. State diagram of ${}^{(\chi,\psi)}\mathbf{S}_H(\rho)$.

The supervisor of the disjunctive architecture of (7) is modified as follows

$$ \mathbf{S}_{H,F}(\rho)={}^{1}\mathbf{S}_H(\rho)\sqcup{}^{3}\mathbf{S}_H(\rho)\sqcup\left(\bigsqcup_{(\chi,\psi)\in\left(\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}\right)-\{(V,\upsilon_H(\rho))\}}{}^{(\chi,\psi)}\mathbf{S}_H(\rho)\right);\ \rho\in\{1,...,n_L/2\}. \tag{10} $$

The alphabet of $\mathbf{S}_{H,F}(\rho)$ is

$$ \mathbb{E}_{S,H,F}(\rho)={}^{1}\mathbb{E}_{S,H}(\rho)\cup{}^{3}\mathbb{E}_{S,H}(\rho)\cup\left(\bigcup_{(\chi,\psi)\in\left(\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}\right)-\{(V,\upsilon_H(\rho))\}}{}^{(\chi,\psi)}\mathbb{E}_{S,H}(\rho)\right). $$

6.3 Decentralized Architecture of the Controlled Water Distribution Network with Faults

Considering actuator and sensor faults related to the ρ-th pair, where $\rho=1,...,n_L/2$, the model corresponding to this pair is computed to be

$$ \mathbf{G}_F(\rho)=\mathop{\|}_{(i,j)\in\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}}\mathbf{G}_{F,i,j} $$

The marked language of the automaton of the ρ -th pair of tanks is computed to be

$$\mathbb{L}_m(\mathbf{G}_F(\rho)) = \bigcap_{(i,j)\in\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}} P_{F,i,j}^{-1}\left(\mathbb{L}_m(\mathbf{G}_{F,i,j})\right)$$

where $P_{F,i,j}$ is the projection of $\mathbb{E}_{F,i,j}^*$ to $\mathbb{E}_{F,\rho}^*$ and $\mathbb{E}_{F,\rho} = \bigcup_{\left((i,j)\in\mathbb{D}_{2\rho-1}\right)\vee\left((i,j)\in\mathbb{D}_{2\rho}\right)} \mathbb{E}_{F,i,j}$. The controlled automaton of $\mathbf{G}_F(\rho)$ is determined to be

$$\mathbf{G}_{F,c}(\rho) = \mathbf{G}_F(\rho)\|\mathbf{S}_{H,F}(\rho)\|$$
$$\left(\|_{\zeta\in\{I,D\}}\left(\left(\|_{(\chi,\psi)\in\mathbb{D}_{\zeta,2\rho-1}}\mathbf{S}_{\zeta,2\rho-1}(\chi,\psi)\right)\|\left(\|_{(\chi,\psi)\in\mathbb{D}_{\zeta,2\rho}}\mathbf{S}_{\zeta,2\rho}(\chi,\psi)\right)\right)\right)$$

The marked language of $\mathbf{G}_{F,c}(\rho)$ is

$$\mathbb{L}_m(\mathbf{G}_{F,c}(\rho)) = \mathbb{L}_m(\mathbf{G}_F(\rho)) \cap P_{H,F,\rho}^{-1}\left(\mathbb{L}_m(\mathbf{S}_{H,F}(\rho))\right) \cap$$
$$\bigcap_{\zeta\in\{I,D\}}\left(\left(\bigcap_{(\chi,\psi)\in\mathbb{D}_{\zeta,2\rho-1}}\left(P_{F,\zeta,2\rho-1}^{-1}(\chi,\psi)\left(\mathbb{K}_{\zeta,2\rho-1}(\chi,\psi)\right)\right)\right)\right) \cap$$
$$\bigcap_{\zeta\in\{I,D\}}\left(\left(\bigcap_{(\chi,\psi)\in\mathbb{D}_{\zeta,2\rho}}\left(P_{F,\zeta,2\rho}^{-1}(\chi,\psi)\left(\mathbb{K}_{\zeta,2\rho}(\chi,\psi)\right)\right)\right)\right)$$

where $P_{H,F,\rho}$ is the projection of $\mathbb{E}_{S,H,F}^*(\rho)$ to $\mathbb{E}_{F,\rho}^*$, $P_{F,\zeta,2\rho-1}(\chi,\psi)$ is the projection of $\mathbb{E}_{S,\zeta,2\rho-1}^*(\chi,\psi)$ to $\mathbb{E}_{F,\rho}^*$ and $P_{F,\zeta,2\rho}(\chi,\psi)$ is the projection of $\mathbb{E}_{S,\zeta,2\rho}^*(\chi,\psi)$ to $\mathbb{E}_{F,\rho}^*$.

The total controlled automaton of the WDN in the presence of faults is

$$\tilde{\mathbf{G}}_{F,c} = \|_{\rho=1}^{n_L/2}\mathbf{G}_{F,c}(\rho).$$

The marked language of $\tilde{\mathbf{G}}_{F,c}$ is

$$\mathbb{L}_m(\tilde{\mathbf{G}}_{F,c}) = \bigcap_{\rho=1}^{n_L/2} P_{F,\rho}^{-1}\left(\mathbb{L}_m(\mathbf{G}_{F,c}(\rho))\right)$$

where $P_{F,\rho}$ is the projection of $\mathbb{E}_{F,\rho}^*$ to $\mathbb{E}_F^*$, where $\mathbb{E}_F = \bigcup_{\rho=1}^{n_L/2}\mathbb{E}_{F,\rho}$.

Remark 4: The nonblocking property of the controlled automaton can be easily proved using Remark 3.

Remark 5: The supervisor control architecture proposed in Sections 5 and the resilient supervisor architecture proposed in Section 6 can be easily implemented using Ladder diagrams or Structured Text ([26], [34]) for PLC/SCADA, or JavaScript [35] for Edge computing implementation. Hence, the control architecture can be implemented to the PLC or the SCADA system of HYDRA testbed (see [17]-[21]).

7 Conclusion

The DES models of all devices (actuators and sensors) of a WDN testbed have been expressed parametrically, as separate DES models. The desired performance of the testbed has been expressed in the form of three rules including all actuators (vertical and horizontal) and sensors. The rules have been translated into a set of regular languages, being parametric to the number of devices of the tank. Each regular language has been realized as a two-state automaton supervisor. The nonblocking property of the controlled automaton and PR of the supervisor scheme have been proved. Next, in the presence of actuator and sensor faults, appropriate PR and nonblocking supervisors have been developed

Implementation of the present supervisor scheme to a cloud-based environment [36] is under investigation.

Acknowledgment

This work was conducted within the "SUB1.1 Clusters of Research Excellence (CREs)" Action of the National Recovery and Resilience Plan "Greece 2.0", co-funded by Greece and the European Union – NextGenerationEU, under the project "Development of Soft Sensors in Water Distribution Networks (ΥΠ3ΤΑ-0560428-DeSw)".

References

1. Zhang, K., Shi, Y., Karnouskos, S., Sauter, T., Fang, H., Colombo, A.W.: Advancements in Industrial Cyber-Physical Systems: An Overview and Perspectives. IEEE Transactions on Industrial Informatics. **19**(1), 716–729 (2023)
2. Henriques, J., Caldeira, F., Cruz, T., Simões, P.: A survey on forensics and compliance auditing for critical infrastructure protection. IEEE Access **12**, 2409–2444 (2024)
3. Grady, C., Rajtmajer, S., Dennis, L.: When smart systems fail: The ethics of cyber–physical critical infrastructure risk. IEEE Transactions Technology and Society, **2**(1), 6–14 (2021)
4. Wonham, W.M., Kai, C.: *Supervisory Control of Discrete-Event Systems*. Springer, Cham (2019)
5. Casandras, C.G., Lafortune, S.: *Introduction to Discrete Event Systems*, 3rd edn. Springer, Cham (2021)
6. Cai, K., Wonham, W.M.: Supervisor localization: A top-down approach to distributed control of discrete-event systems. IEEE Transactions on Automatic Control **55**(3), 605–618 (2010)
7. Mohajerani, S., Malik, R., Fabian, M.: A framework for compositional synthesis of modular nonblocking supervisors. IEEE Transactions on Automatic Control **59**(1), 150–162 (2014)
8. Koumboulis, F.N., Fragkoulis, D.G., Siake, B.: Safe operation of a modular production system via supervisor automata. In: Proc. 2023 31st Mediterranean Conference on Control and Automation (MED), pp. 938–945. IEEE, Limassol (2023)
9. Fragkoulis, D. G., Koumboulis, F. N., Tzamtzi, M. P., Totomis, P. G.: Event-based supervisor control for a cyber-physical waterway lock system. Computer-Aided Civil and Infrastructure Engineering, **40**(9), 1189-1207 (2025)

10. Yadav, G., Paul, K.: Architecture and security of SCADA systems: A review. International Journal of Critical Infrastructure Protection **34**, 100433 (2021)
11. Gaggero, G.B., Armellin, A., Portomauro, G., Marchese, M.: Industrial Control System-Anomaly Detection Dataset (ICS-ADD) for Cyber-Physical Security Monitoring in Smart Industry Environments. IEEE Access **12**, 64140–64149 (2024)
12. Alanazi, M., Mahmood, A., Chowdhury, M.J.M.: SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. Computers & Security **125**, 103028 (2023)
13. Wang, Z., Zhang, Y., Chen, Y., Liu, H., Wang, B., Wang, C.: A survey on programmable logic controller vulnerabilities, attacks, detections, and forensics. Processes **11**(3), 918 (2023)
14. Vrachimis, S., Santra, S., Agathokleous, A., Pavlou, P., Kyriakou, M., Psaras, M., Eliades, D.G., Polycarpou, M.M.: WaterSafe: A water network benchmark for fault diagnosis research. IFAC-Pap. OnLine **55**(6), 655–660 (2022)
15. Creaco, E., Campisano, A., Fontana, N., Marini, G., Page, P.R., Walski, T.: Real time control of water distribution networks: A state-of-the-art review. Water Res. **161**, 517–530 (2019)
16. Oberascher, M., Rauch, W., Sitzenfrei, R.: Towards a smart water city: A comprehensive review of applications, data requirements, and communication technologies for integrated management. Sustainable Cities and Society **76**, 103442 (2022)
17. HYDRA testbed repository, https://github.com/hydra-testbed/, last accessed 2025/05/17.
18. Bernieri, G., Del Moro, F., Faramondi, L., Pascucci, F.: A testbed for integrated fault diagnosis and cyber security investigation. In: Proceedings of the 2016 International Conference on Control, Decision and Information Technologies (CoDIT), pp. 454–459. IEEE, Saint Julian's (2016)
19. Bernieri, G., Damiani, S., Del Moro, F., Faramondi, L., Pascucci, F., Tambone, F.: A Multiple-Criteria Decision Making method as support for critical infrastructure protection and Intrusion Detection System. In: Proceedings IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society, pp. 4871–4876. IEEE, Florence (2016)
20. Battisti, F., Bernieri, G., Carli, M., Lopardo, M., Pascucci, F.: Detecting integrity attacks in IoT-based cyber physical systems: a case study on Hydra testbed. In: 2018 Global Internet Things Summit (GIoTS), pp. 1–6. IEEE, Bilbao (2018)
21. Melo, J.A.S.: Opacity-Based Defense for Deterministic Finite Automata Against Passive and Actuator-Enablement Attacks. Master's Thesis, University of Coimbra, Portugal (2024)
22. Fragkoulis, D.G., Koumboulis, F.N.: Supervisor Water Level Control for the Tanks in a Modular Water Distribution Network Testbed. In: 29th International Conference on Intelligent Engineering Systems 2025 (INES 2025). IEEE, Palermo (2025)
23. Koumboulis, F.N., Fragkoulis, D.G., Georgakopoulos, P.: A Distributed Supervisor architecture for a General Wafer Production System. Sensors **23**(9), 4545 (2023)
24. Koumboulis, F.N., Fragkoulis, D.G., Arapakis, S.: Supervisor design for an assembly line in the presence of faults. In: Proceedings of IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–8. IEEE, Stuttgart (2022)
25. Vieira, A.D., Santos, E.A.P., de Queiroz, M.H., Leal, A.B., de Paula Neto, A.D., Cury, J.E.R.: A method for PLC implementation of supervisory control of discrete event systems. IEEE Transactions Control Syst. Technol. **25**(1), 175–191 (2017)
26. Menexis, A.N., Koumboulis, F.N., Fragkoulis, D.G., Kouvakas, N.D.: Toward design and implementation of intelligent manufacturing in semiconductor production industry with wafer chamber faults. In: Frontiers of Artificial Intelligence, Ethics, and Multidisciplinary Applications (FAIEMA 2023), Springer, Singapore (2023)

27. Koumboulis, F.N., Fragkoulis, D.G.: Input-output supervisor design for systems analyzed in cooperating pairs of subsystems. In: Proceedings of the 2024 32nd Mediterranean Conference on Control and Automation (MED), pp. 43–49. IEEE, Chania (2024)
28. Yang, Y., Xu, E., Shi, Y., Jia, T., Ren, Y., Yang, H., Li, Y.: Current status and applications for hydraulic pump fault diagnosis: A review. Sensors **22**(24), 9714 (2022)
29. Zhong, Q., Xu, E., Shi, Y., Jia, T., Ren, Y., Yang, H., Li, Y.: Fault diagnosis of the hydraulic valve using a novel semi-supervised learning method based on multi-sensor information fusion. Mechanical Systems and Signal Processing **189**, 110093 (2023)
30. Li, D., Wang, Y., Wang, J., Wang, C., Duan, Y.: Recent advances in sensor fault diagnosis: A review. Sensors and Actuators A: Physical **309**, 111990 (2020)
31. Lafortune, S., Lin, F., Hadjicostis, C.N.: On the history of diagnosability and opacity in discrete event systems. Annual Reviews in Control **45**, 257–266 (2018)
32. Yoo, T.S., Lafortune, S.: A general architecture for decentralized supervisory control of discrete-event systems. Discrete Event Dynamic Systems **12**, 335-377 (2002)
33. Liu, F., Lin, H.: "Reliable supervisory control for general architecture of decentralized discrete event systems," Automatica **46**(9), 1510-1516 (2010)
34. Vieira, A.D., Santos, E.A.P., de Queiroz, M.H., Leal, A.B., de Paula Neto, A.D., Cury, J.E.R.: A method for PLC implementation of supervisory control of discrete event systems. EEE Transactions on Control Systems Technology **25**(1), 175–191 (2017)
35. Fragkoulis, D.G., Koumboulis, F.N., Menexis, A.N.: Edge Computing for Safe Control of a Parametric Multi-floor Manufacturing Process. In: 29th International Conference on Intelligent Engineering Systems 2025 (INES 2025), IEEE, Palermo (2025)
36. Menexis, A.N., Fragkoulis, D.G., Koumboulis, F.N., Skarpetis, M.G.: A FIWARE based Input-Output Supervisor Control Implementation. In: IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 01–04. IEEE (2024)