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

Dimitrios G. Fragkoulis, Fotis N. Koumboulis,
Maria P. Tzamtzi and Nikolaos D. Kouvakas

Robotics, Automatic Control and
Cyber-Physical Systems Laboratory,
Department of Digital Industry Technologies,
School of Science,
National and Kapodistrian University of Athens
Greece

Greece 2.0
NATIONAL RECOVERY AND RESILIENCE PLAN
Funded by the European Union
NextGenerationEU

Introduction

- Water Distribution Networks (WDNs) play a fundamental role in sustaining modern life providing clean and safe water for residential, commercial, and industrial use ([1]).
- The main parts of WDNs are reservoirs, pumping stations, treatment facilities, and pipelines.
- All parts of a WDN rely on automated control systems to ensure efficient operation ([2], [3]).
- Discrete Event Systems (DES) and Supervisor Control Theory (SCT) ([4]) provide the background for the development of efficient coordinating tools for CPS ([5]) such as WDNs.

---

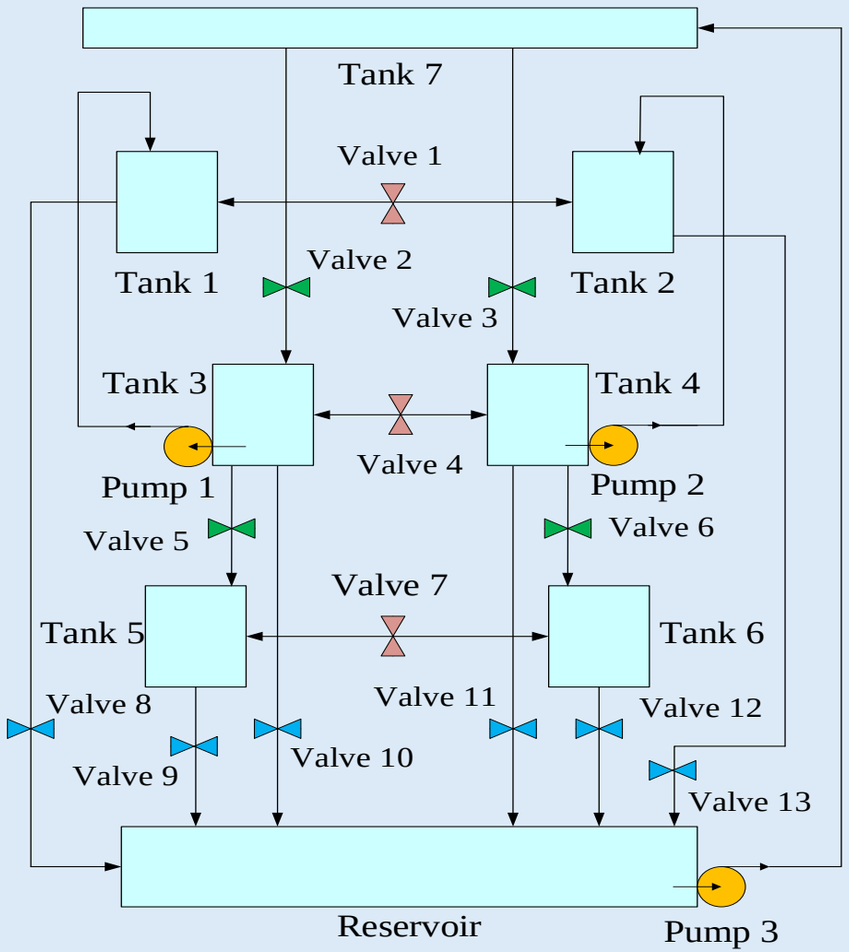
1. Creaco, E., Campisano, A., Fontana, N., Marini, G., Page, P.R., Walski, T.: Real time control of water distribution networks: A state-of-the-art review. Water Res. 161, 517–530 (2019)
2. Vrachimis, S., Santra, S., Agathokleous, A., Pavlou, P., Kyriakou, M., Psaras, M., Eliades, D.G., Polycarpou, M.M.: WaterSafe: A water network benchmark for fault diagnosis research. IFAC-Pap. OnLine 55(6), 655–660 (2022)
3. 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)
4. Wonham, W.M., Kai, C.: Supervisory Control of Discrete-Event Systems. Springer, Cham (2019).
5. 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)

Scope of the present work

- A usual WDN comprises large numbers of tanks distributed in several levels.
- The flow of the water between these tanks is achieved with the use of appropriate valves and pumps
- Controlling the operation of the valves and pumps aims to achieve efficient and safe operation of the WDN, namely efficient response to several demand patterns, overflow avoidance and fault resilience
- Scope of the present paper is to propose a supervisory control scheme that uses sensor and actuator signals in order to contribute toward the following goals:
  - Retain the level within each tank within desired upper and low limits
  - Retain the efficient performance of the WDN, even in the presence of sensor and actuator faults
- The proposed supervisory scheme is presented for a WDN testbed (HYDRA testbed [6]), covering various WDNs architectures and functionalities.

6. HYDRA testbed repository, https://github.com/hydra-testbed/, last accessed 2025/05/17.

Description of the Testbed



- The HYDRA testbed features a modular cyber-physical architecture that emulates many real-world WDNs.
- At the top, there is a large tank simulating a typical water tower.
- There are 6 additional tanks distributed across three distinct levels.
- Each tank is equipped with a water level sensor (ultrasonic).
- At the base, there lies a reservoir, symbolizing an aquifer.
- The tanks are interconnected through non-pressurized piping, allowing gravity-driven water flow aided by pumps (3 pumps).
- The system incorporates ten electromechanical valves.
- The green colored valves represent the consumption ending in the tank of a lower level.
- The blue colored valves represent the consumption (or leakages).
- The red valves enable inter-tank connections.

Outline of the Paper

- The DES models of the actuators and sensors are expressed parametrically
- The desired performance of the WDN is expressed in the form of three rules
- The rules are translated to a set of regular languages (parametric with respect to the number of devices of the tank)
- Each regular language is realized by a two-state finite deterministic supervisor automaton
- A hybrid supervisor control architecture is proposed (disjunctive - conjunctive architecture), that implements the rules, thus imposing the desired performance to the WDN
- The necessary properties of the developed supervisor scheme will be proved
- The DES models of the devices in the presence of fault are presented
- A hybrid resilient supervisor control architecture is proposed, satisfying desired operation in the presence of faults

A Generalized WDN Configuration (1/2)

- Total number of tanks: $n_L \rightarrow$ Total number of water level sensors: n_L
- Total number of pumps: n_P
- Total number of valves: n_V
- $k \in \{1,...,n_L\}$: index of each tank and each level sensor
- (i, j), $i \in \{P,V,L\}$, $j \in \{1,...,n_i\}$: pair denoting an actuator or sensor of the WDN

- The tanks are grouped into pairs of the form $(2\rho-1, 2\rho)$, indexed by $\rho \in \{1,...,, n_L / 2\}$
- The k –th tank belongs to the ρ –th pair, where

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

- The tanks of each pair are connected through a horizontal valve

Hydra testbed

$$n_L = 6,\ n_P = 2,\ n_V = 13$$

The pairs of tanks are $\rho = 1 \rightarrow (1,2)$, $\rho = 2 \rightarrow (3,4)$, $\rho = 3 \rightarrow (5,6)$.

A Generalized WDN Configuration (2/2)

For the k-th tank:

- $\mathbb{D}_k$: the set containing all pairs of the forms (i, j), $i \in \{P, V, L\}$, $j \in \{1, ..., n_i\}$
- $\ell_k = |\mathbb{D}_k|$: the total number of devices of the k-th tank
- $\mathbb{D}_{I,k}$: set of pairs (i, j) denoting vertical actuators contributing to the water level increase of the tank
- $\mathbb{D}_{D,k}$: set of pairs (i, j) denoting vertical actuators contributing to the water level decrease of the tank
- $\mathbb{D}_{H,k}$: contains the pair denoting the horizontal valve of the tank

$$\mathbb{D}_{H,2\rho-1} = \mathbb{D}_{H,2\rho},\ \left|\mathbb{D}_{H,2\rho-1}\right| = 1,\ \rho \in \{1, ..., n_L / 2\}$$

The horizontal valve connecting the tanks of the $\rho-$th pair can be expressed in the form:

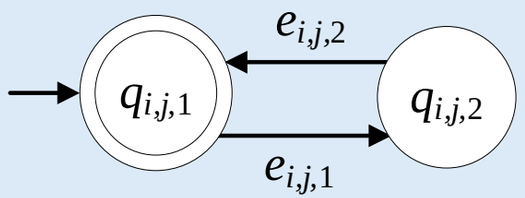
$$\left(V, \upsilon_H(\rho)\right) = (V, \xi) \in \mathbb{D}_{H,2\rho-1};\ \rho \in \{1, ..., n_L / 2\}$$

Example:

For Tank 1:

$\mathbb{D}_1 = \{(L,1),(P,1),(V,1),(V,8)\}$, $\mathbb{D}_{I,1} = \{(P,1)\}$, $\mathbb{D}_{D,1} = \{(V,8)\}$, $\mathbb{D}_{H,1} = \{(V,1)\}$, $\rho = 1$ and $\mathbb{D}_{H,2} = \{(V,1)\}$.

DES Models of the Actuators (Pumps/Valves)



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

State set: $\mathbb{Q}_{i,j} = \{q_{i,j,1}, q_{i,j,2}\}$;

- $q_{i,j,1}$**: idle (non-working) mode,** $q_{i,j,2}$**: working mode**

Initial state $x_{i,j,0} = q_{i,j,1}$, Marked states set $\mathbb{Q}_{i,j,m} = \{q_{i,j,1}\}$

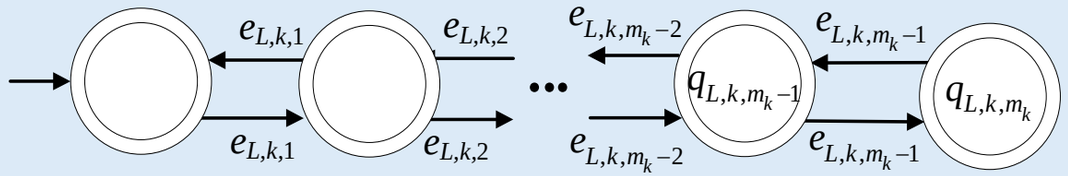
Alphabet $\mathbb{E}_{i,j} = \{e_{i,j,1}, e_{i,j,2}\}$, $\mathbb{E}_{i,j,c} = \{e_{i,j,1}, e_{i,j,2}\}$, $\mathbb{E}_{i,j,uc} = \varnothing$

- $e_{i,j,1}$**: command to activate the device,** $e_{i,j,2}$**: command to deactivate the device**

Marked Behavior: $\mathbb{L}_m(\mathbf{G}_{i,j}) = (e_{i,j,1}e_{i,j,2})^*$

$\mathbf{G}_{i,j}$ is nonblocking.

Model of the Water Level Sensors



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

State set: $\mathbb{Q}_{L,k} = \{q_{L,k,1},\ldots,q_{L,k,m_k}\}$;

- $q_{L,k,\mu}$, $\mu \in \{1,\ldots,m_k-1\}$**: the μ-th zone's level (the level of the water is between the lower limit and the upper limit of the zone)**
- q_{L,k,m_k}**: the water level is higher than the upper limit of the m_k-1 zone**

Initial state $x_{L,k,0} = q_{L,k,1}$, Marked states set $\mathbb{Q}_{L,k,m} = \mathbb{Q}_{L,k}$

Alphabet $\mathbb{E}_{L,k} = \{e_{L,k,1},\ldots,e_{L,k,m_k-1}\}$, $\mathbb{E}_{L,k,c} = \varnothing$, $\mathbb{E}_{L,k,uc} = \{e_{L,k,1},\ldots,e_{L,k,m_k-1}\}$.

- $e_{L,k,\mu}$, $\mu \in \{1,\ldots,m_k-1\}$**: the water level is approaching the upper limit of the μ-th zone**

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

Model of Faults

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

State set: $\mathbb{Q}_{E,i,j} = \{q_{E,i,j,1}, q_{E,i,j,2}\}$;

- $q_{E,i,j,1}$**: the non-faulty case,** $q_{E,i,j,2}$**: the faulty case**

Initial state $x_{E,i,j,0} = q_{E,i,j,1}$, Marked states set $\mathbb{Q}_{E,i,j,m} = \{q_{E,i,j,1}\}$.

Alphabet: $\mathbb{E}_{E,i,j} = \{e_{E,i,j,1}, e_{E,i,j,2}\}$, $\mathbb{E}_{E,i,j,c} = \varnothing$, $\mathbb{E}_{E,i,j,uc} = \mathbb{E}_{E,i,j}$.

- $e_{E,i,j,1}$**: the signal that a fault has been detected**
- $e_{E,i,j,2}$**: the signal that the fault has been repaired**

Marked Behavior: $\mathbb{L}_m(\mathbf{G}_{E,i,j}) = (e_{E,i,j,1} e_{E,i,j,2})^*$

$\mathbf{G}_{RC}$ is nonblocking.

Models of the Devices in the Presence of Faults

Model of each device in the presence of faults: $\mathbf{G}_{F,i,j} = \mathbf{G}_{i,j} \,||\, \mathbf{G}_{E,i,j}$, $i \in \{P,V,L\} \wedge j \in \{1,...,n_i\}$

The set of the states: $\mathbb{Q}_{F,i,j} = \mathbb{Q}_{i,j} \times \mathbb{Q}_{E,i,j}$.

The alphabet: $\mathbb{E}_{F,i,j} = \mathbb{E}_{i,j} \cup \mathbb{E}_{E,i,j}$,

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

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.

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). 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.

Desired Behavior of the WDN without Faults (1/2)

- The WDN must preserve the desired water level within the tanks
- The water level must be above a predefined zone and at the same time must not exceed the upper limit.
- The actuators of the WDN, responsible for the rise and drop of the water level, must be controlled to guarantee the desired level.

Example:
In case the water level of a tank is above the upper limit then:

1. The valves responsible for the rise of the water level (valves above the tank) and the pump (if any) must stay closed.
2. The corresponding horizontal valve can open, to send water to the pairing tank.

In case the water level of a tank is below the lower limit then:

3. The valves responsible for the decrease of the water level (valves below the tank) must stay closed.
4. The corresponding horizontal valve can open, to get water from the pairing tank.

Desired Behavior of the WDN without Faults (2/2)

The rules describing the desired behavior of the actuators:

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 $\rho \in \{1,...,n_L/2\}$, 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 in "disable event form" and the third rule is in "enable event form".

Regular Languages without Faults

Rule 1, for the k-th tank, $k \in \{1,...,n_L\}$ and the vertical actuator $(\chi,\psi) \in \mathbb{D}_{I,k}$:

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

Rule 2, for the k-th tank, $k \in \{1,...,n_L\}$ and the vertical actuator $(\chi,\psi) \in \mathbb{D}_{D,k}$:

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

Rule 3 for the horizontal valve $\left(V, \upsilon_H(\rho)\right)$ is analyzed in four cases:

- Case 1 (the 2ρ-th tank's level is between its minimum and its maximum value):

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

- Cases 2/4 (the 2ρ-th/$2\rho-1$-th tank's level is below its minimum value or above its maximum value:

$$^2\mathbb{K}_H(\rho) = {}^4\mathbb{K}_H(\rho) = e^*_{V,\upsilon_H(\rho),1}.$$

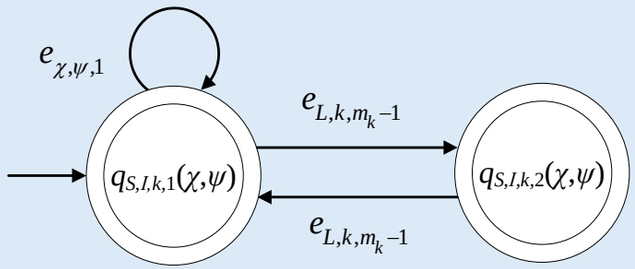
- Case 3 (the $2\rho-1$-th tank's level is between its minimum and its maximum value):

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

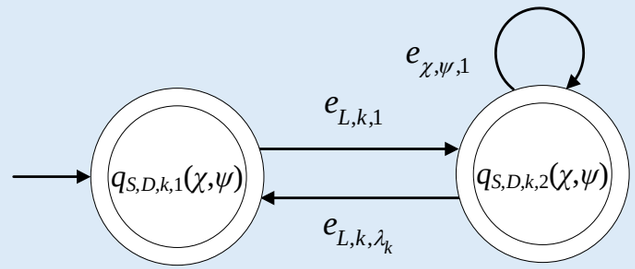
Supervisors of the WDN without Faults (1/2)

- $\mathbf{S}_{I,k}(\chi,\psi)$: the supervisor realizing $\mathbb{K}_{I,k}(\chi,\psi)$, $k \in \{1,...,n_L\}$ $(\chi,\psi) \in \mathbb{D}_{I,k}$
- $\mathbb{E}_{S,I,k}(\chi,\psi) = \{e_{\chi,\psi,1}, e_{L,k,m_k-1}\}$: alphabet of $\mathbf{S}_{I,k}(\chi,\psi)$
- $\mathbf{S}_{D,k}(\chi,\psi)$: supervisor realizing $\mathbb{K}_{D,k}(\chi,\psi)$, $k \in \{1,...,n_L\}$ $(\chi,\psi) \in \mathbb{D}_{D,k}$
- $\mathbb{E}_{S,D,k}(\chi,\psi) = \{e_{\chi,\psi,1}, e_{L,k,1}\}$: alphabet of $\mathbf{S}_{D,k}(\chi,\psi)$

$\mathbf{S}_{I,k}(\chi,\psi)$



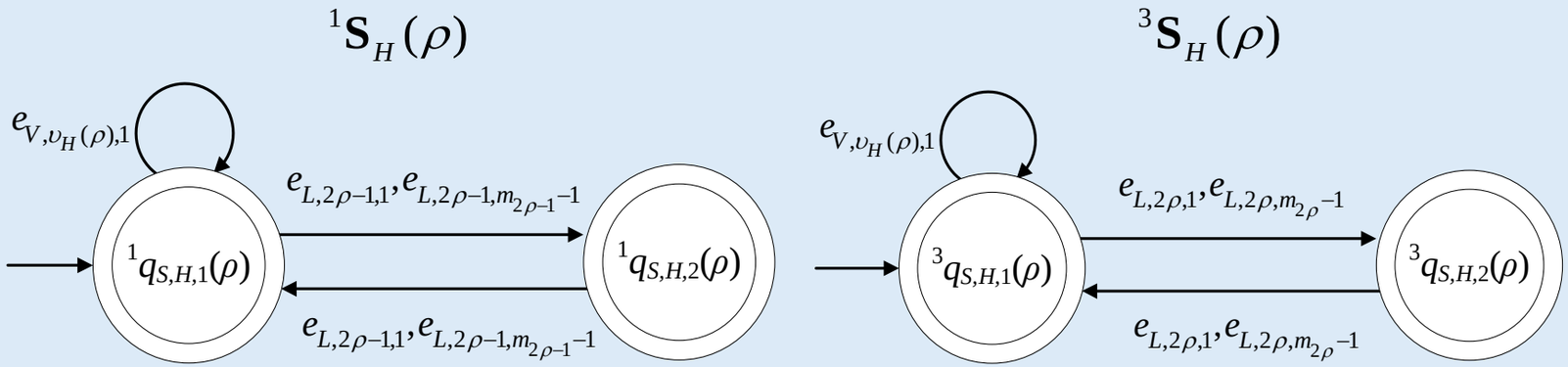
$\mathbf{S}_{D,k}(\chi,\psi)$



The vertical actuators are restricted by the 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**.

Supervisors of the WDN without Faults (2/2)

- ${}^{1}\mathbf{S}_{H}(\rho)$: supervisor realizing ${}^{1}\mathbb{K}_{H}(\rho)$
- ${}^{1}\mathbb{E}_{S,H}(\rho)=\{e_{V,\upsilon_H(\rho),1}, e_{L,2\rho-1,1}, e_{L,2\rho-1,m_{2\rho-1}-1}\}$: alphabet of ${}^{1}\mathbf{S}_{H}(\rho)$
- ${}^{3}\mathbf{S}_{H}(\rho)$: supervisor realizing ${}^{3}\mathbb{K}_{H}(\rho)$
- ${}^{3}\mathbb{E}_{S,H}(\rho)=\{e_{V,\upsilon_H(\rho),1}, e_{L,2\rho,1}, e_{L,2\rho,m_{2\rho}-1}\}$: alphabet of ${}^{3}\mathbf{S}_{H}(\rho)$



Physical Realizability (PR) of $\mathbf{S}_{I,k}(\chi,\psi)$, $\mathbf{S}_{D,k}(\chi,\psi)$, ${}^{1}\mathbf{S}_{H}(\rho)$ and ${}^{3}\mathbf{S}_{H}(\rho)$ is proved

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.
- **If at least one of $^{1}\mathbf{S}_{H}(\rho)$ and $^{3}\mathbf{S}_{H}(\rho)$ permits the event that opens the valve to take place, then the event is permitted to take place.**
- This requirement is expressed as a **disjunctive architecture** of the supervisors $^{1}\mathbf{S}_{H}(\rho)$ and $^{3}\mathbf{S}_{H}(\rho)$

$$\mathbf{S}_{H}(\rho) = {}^{1}\mathbf{S}_{H}(\rho) \llcorner\!\lrcorner {}^{3}\mathbf{S}_{H}(\rho);\ \rho \in \{1,\ldots,n_{L}/2\}$$

- 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.
- The alphabet of $\mathbf{S}_{H}(\rho)$ is $\mathbb{E}_{S,H}(\rho) = {}^{1}\mathbb{E}_{S,H}(\rho) \cup {}^{3}\mathbb{E}_{S,H}(\rho)$.

Decentralized Architecture of the Controlled WDN without Faults (1/3)

- **The automaton of the ρ-th pair of tanks**: $\mathbf{G}(\rho) = \|_{(i,j)\in\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}} \mathbf{G}_{i,j}$

- The **marked language** of the automaton of the ρ-th pair of tanks: $\mathbb{L}_m(\mathbf{G}(\rho)) = \bigcap_{(i,j)\in\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}} P_{i,j}^{-1}\left(\mathbb{L}_m(\mathbf{G}_{i,j})\right)$

  - $P_{i,j}$: the projection of $\mathbb{E}_{i,j}^*$ to $\mathbb{E}^*(\rho)$
  - $\mathbb{E}(\rho) = \bigcup_{(i,j)\in\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}} \mathbb{E}_{i,j}$.

- **The controlled automaton of $\mathbf{G}(\rho)$, $\rho = 1,\ldots,n_L/2$:**

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

Decentralized Architecture of the Controlled WDN without Faults (2/3)

- **The marked language of $\mathbf{G}_c(\rho)$:**

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

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

  - $P_{\zeta,2\rho-1}(\chi,\psi)$, $P_{\zeta,2\rho}(\chi,\psi)$, $P_{H,\rho}$: projections of $\mathbb{E}^*_{S,\zeta,2\rho-1}(\chi,\psi)$, $\mathbb{E}^*_{S,\zeta,2\rho}(\chi,\psi)$, $\mathbb{E}^*_{S,H}(\rho)$ to $\mathbb{E}^*(\rho)$
  - $\mathbb{E}_{S,\zeta,k}(\chi,\psi)$: the alphabet of the language $\mathbb{K}_{\zeta,k}(\chi,\psi)$, $\zeta\in\{I,D\}$

- **The total controlled automaton of the WDN: $\tilde{\mathbf{G}}_c = \|_{\rho=1}^{n_L/2}\mathbf{G}_c(\rho)$**

Decentralized Architecture of the Controlled WDN without Faults (3/3)

- The **marked language** of $\tilde{\mathbf{G}}_c$: $\mathbb{L}_m(\tilde{\mathbf{G}}_c) = \bigcap_{\rho=1}^{n_L/2} P_\rho^{-1}\left(\mathbb{L}_m(\mathbf{G}_c(\rho))\right)$
  - P_ρ : the projection of $\mathbb{E}^*(\rho)$ to $\mathbb{E}^*$, where $\mathbb{E} = \bigcup_{\rho=1}^{n_L/2} \mathbb{E}(\rho)$.

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.

Behavior of the WDN with Faults

- In case of actuator and/or sensor faults, then the supervisor design of the horizontal valves must include the possible faults.
- If a valve or a pump stuck (open or close) the horizontal valve of the corresponding tank must be able to open in order to send or receive water from the pairing tank.

A new and extended version of 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 $\left(V,\upsilon_H(\rho)\right)$ valve, is in fault, then the corresponding horizontal valve $\left(V,\upsilon_H(\rho)\right)$ is allowed to be activated.

The rules, regular languages and supervisors of Rules 1 and 2 remain the same as in the no faulty case

Regular Languages with Faults

The desired behavior for the ρ-th pair of tanks is studied for the following cases:

- The four cases of the not faulty behavior
- Additional cases, each corresponding to the presence of faults in one of the actuators/sensors indexed by:

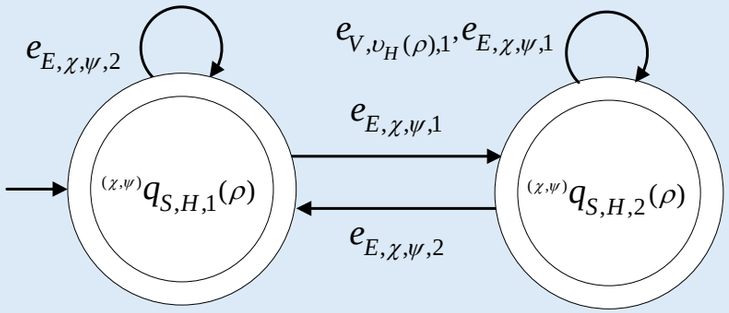
$$(\chi,\psi)\in\left(\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}\right)-\left\{\left(V,\upsilon_H(\rho)\right)\right\}$$

Desired behavior for each additional case:

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

Resilient Supervisor of the WDN

- ${}^{(\chi,\psi)}\mathbf{S}_H(\rho)$: supervisor realizing ${}^{(\chi,\psi)}\mathbb{K}_H(\rho)$
- ${}^{(\chi,\psi)}\mathbb{E}_{S,H}(\rho)=\{e_{V,\upsilon_H(\rho),1}, e_{E,\chi,\psi,1}, e_{E,\chi,\psi,2}\}$: alphabet of ${}^{(\chi,\psi)}\mathbf{S}_H(\rho)$
- Physical realizability of ${}^{(\chi,\psi)}\mathbf{S}_H(\rho)$ is proved



Modified disjunctive architecture taking into account faults:

$$\mathbf{S}_{H,F}(\rho)={}^{1}\mathbf{S}_H(\rho)\llcorner\!\lrcorner{}^{3}\mathbf{S}_H(\rho)\llcorner\!\lrcorner\left(\underset{(\chi,\psi)\in\left(\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}\right)-\{(V,\upsilon_H(\rho))\}}{\llcorner\!\lrcorner}{}^{(\chi,\psi)}\mathbf{S}_H(\rho)\right);\rho\in\{1,\ldots,n_L/2\}$$

Alphabet of $\mathbf{S}_{H,F}(\rho)$: $\mathbb{E}_{S,H,F}(\rho)={}^{1}\mathbb{E}_{S,H}(\rho)\cup{}^{3}\mathbb{E}_{S,H}(\rho)\cup\left(\underset{(\chi,\psi)\in\left(\mathbb{D}_{2\rho-1}\cup\mathbb{D}_{2\rho}\right)-\{(V,\upsilon_H(\rho))\}}{\bigcup}{}^{(\chi,\psi)}\mathbb{E}_{S,H}(\rho)\right)$

Decentralized Architecture of the Controlled WDN with Faults (1/3)

- **Model of the ρ-th pair in the presence of faults:**

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

- **Marked language** of $\mathbf{G}_F(\rho)$:

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

  - $P_{F,i,j}$: the projection of $\mathbb{E}_{F,i,j}^*$ to $\mathbb{E}_{F,\rho}^*$, $\mathbb{E}_{F,\rho} = \bigcup_{\left((i,j)\in\mathbb{D}_{2\rho-1}\right)\vee\left((i,j)\in\mathbb{D}_{2\rho}\right)} \mathbb{E}_{F,i,j}$.

- **Controlled automaton** of $\mathbf{G}_F(\rho)$:

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

Decentralized Architecture of the Controlled WDN with Faults (2/3)

- **Marked language** of $\mathbf{G}_{F,c}(\rho)$:

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

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

  - $P_{H,F,\rho}, P_{F,\zeta,k}(\chi,\psi)$: projections of $\mathbb{E}^*_{S,H,F}(\rho)$, $\mathbb{E}^*_{S,\zeta,k}(\chi,\psi)$ to $\mathbb{E}^*_{F,\rho}$.

- **Total controlled automaton of the WDN in the presence of faults:**

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

Decentralized Architecture of the Controlled WDN with Faults (3/3)

Marked language of $\tilde{\mathbf{G}}_{F,c}$:

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

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

The nonblocking property of the controlled automaton can be easily proved

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 for PLC/SCADA, or JavaScript for Edge computing implementation. Hence, the control architecture can be implemented to the PLC or the SCADA system of HYDRA testbed.

Conclusion and Perspectives

- The DES models of actuators and sensors of the HYDRA testbed have been expressed parametrically
- The desired performance of the testbed has been expressed in the form of three rules
- 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 Physical Realizability of the supervisor scheme have been proved
- The rules describing the desired performance have been modified taking into account actuator/sensor faults
- In the presence of actuator and sensor faults, appropriate DES models, and PR and nonblocking supervisors have been developed

➢ Implementation of the present supervisor scheme to a cloud-based environment is under investigation