sensors

MDPI

Article

Modular Supervisory Control for the Coordination of a Manufacturing Cell with Observable Faults

Nikolaos D. Kouvakas [1], Fotis N. Koumboulis [1], Dimitrios G. Fragkoulis [2,*] and Aristotelis Souliotis [2]

[1] Department of Digital Industry Technologies, School of Science, National and Kapodistrian University of Athens, Euripus Campus, 34400 Evia, Greece
[2] Core Department, National and Kapodistrian University of Athens, Euripus Campus, 34400 Evia, Greece
* Correspondence: dfragkoulis@uoa.gr

Abstract: In the present paper, a manufacturing cell in the presence of faults, coming from the devices of the process, is considered. The modular modeling of the subsystems of the cell is accomplished using of appropriate finite deterministic automata. The desired functionality of the cell as well as appropriate safety specifications are formulated as eleven desired languages. The desired languages are expressed as regular expressions in analytic forms. The languages are realized in the form of appropriate general type supervisor forms. Using these forms, a modular supervisory design scheme is accomplished providing satisfactory performance in the presence of faults as well guaranteeing the safety requirements. The aim of the present supervisor control scheme is to achieve tolerance of basic characteristics of the process coordination to upper-level faults, despite the presence of low-level faults in the devices of the process. The complexity of the supervisor scheme is computed.

Keywords: industrial processes; discrete event systems; supervisory control; fault tolerant control

check for updates

Citation: Kouvakas, N.D.; Koumboulis, F.N.; Fragkoulis, D.G.; Souliotis, A. Modular Supervisory Control for the Coordination of a Manufacturing Cell with Observable Faults. *Sensors* **2023**, *23*, 163. https://doi.org/10.3390/s23010163

Academic Editors: Francesc Pozo, Mohammad N Noori, Steven Chatterton and Jose Alfonso Antonino-Daviu

Received: 22 November 2022
Revised: 17 December 2022
Accepted: 20 December 2022
Published: 23 December 2022

1. Introduction

In flexible manufacturing systems (FMS), the infrastructure is composed of basic components (robots, computer numerical control (CNC), assembling machines, and storing systems) or islands of components, where each island of components is unreconfigurable. This consideration requires a two-layer control design. In the first layer, the components and/or the islands of components are controlled using the respective local sensors and actuators. The control objective of this layer is to perform specific activities of the subsystem [1]. In the second layer, the control objective is the synchronization/coordination of the individual subsystems to satisfy safety and functionality specifications of the overall manufacturing process [1]. The flexibility of the process results from modification of the second layer controller. Advances in the controller hardware contribute toward this scheme see [2,3]. However, as the Programmable Logic Controllers (PLCs) is one of the main architectures of manufacturing system control the use of formal methods for controller synthesis and PLC program design (with standardized languages, e.g., International Electrotechnical Commission (IEC) 61131-3) is crucial, see [2–5]. Supervisory control theory (SCT) [6] is a formal method that tackles the above problems crossing the bridge between the event-based automation and the synchronous signal-based PLC world, see [1,7]. Most commonly, Ladder Diagrams (for PLCs) are used to implement monolithic or modular supervisors. For the definition of monolithic and modular supervisors, see [6,8]. Monolithic supervisors suffer from state explosion as the models grow. The implementation of a single supervisor with many states could make the control program unreliable and/or even unstable [1]. Modular supervisor design requires on-the-fly synchronization of the plant and the controller [5]. However, it reduces computational complexity by reducing the total number of states [1].

The supervisory control design in the presence of faults of the manufacturing process is of particular importance. Indicatively, see [9,10] and the references therein. In the present paper, it is considered that the sensors and the actuators can fail in any time, and once a sensor fault took place, the fault is permanent and requires repair, see also [10]. Here, a modular modelling and supervisor design method will be applied to a manufacturing cell presented in [1,3,11]. The method is in the Ramadge Wonham framework, see [6,8] and the references therein, being one of the milestones of SCT. The proposed supervisor design is based on the consideration of real time knowledge of the occurrence of faults, see [12], through appropriate sensors and/or diagnosers that accomplish the detection and/or isolation of faults. Regarding fault diagnosis, many methods has been developed. Indicatively, see [13] as well [14–16], where diagnosis methods using discrete event systems (DES) are presented.

In the present paper, a fault driven supervisory control scheme will be designed considering that the faults are a priori defined and are observable by appropriate monitoring systems. The presence of faults may cause discoordination of the process or even damage of devices. For instance, drilling tool wear or tool brake may damage the manufactured product. Also, a fault in the robotic manipulator may cause product overflow on the table. Furthermore, faults in the circular rotating table can cause a material overflow or a material underflow in the cell's components. Such faults may cause serious damages in the manufacturing cell's devices and/or the manufactured products. In general, the presence of faults in the devices of the manufacturing process may cause discoordination of the process, being an upper-level fault of composite type. The present supervisory control scheme aims towards achieving fault tolerance in basic characteristics of the coordination of the process, despite the presence of lower-level faults, namely technical faults in the devices of the process. Thus, the proposed supervisory control scheme guarantees the safety of the system despite the presence of lower-level faults. All unwanted series of actions, that may cause system discoordination, are avoided despite the presence of faults.

According to [17], in modern automation systems, fault handling gains more and more attention. Clearly, an early fault detection and fault treatment may eliminate the undesired sequences caused by the fault. The main motivation of the present work is the avoidance of the malfunctions, usually met in manufacturing of the present type, by forcing the controlled system to stop its evolution before the execution of the undesired sequences, see also [17,18]. The design of a supervisory control scheme for a well-established and experimentally tested manufacturing cell, with many applications (indicatively see [1,3,11]) is another motivation of the present research. Also, for the manufacturing cell at hand, several supervisors, have been implemented in PLC environment and tested, indicatively see [1,3,11]. The above characteristics contribute to the feasibility of the proposed safety oriented supervisory control scheme.

The first contribution of the paper is the modelling of the manufacturing cell in the presence of faults in every subsystem. The second is the presentation of the system's specifications in the form of regular languages, in analytic forms, and the realization of the supervisors controlling the process. It is mentioned that most of the supervisors are realized through general prespecified supervisor forms that facilitate the proof of controllability and nonblocking, as well as PLC implementation. The third contribution of the present paper is the implementation of the proposed supervisor using Ladder Diagrams and function blocks. The final contribution of the paper is the distributed analysis in both modeling and nonblocking supervisory design of the manufacturing cell, providing a clear and sufficient method for future case studies of the present type.

The proposed supervisors have been designed to be as possible maximally permissive, while they guarantee the PR property of the supervisors regarding the total automaton of the manufacturing cell. To accomplish this, all uncontrollable events of a supervisor are required to belong to the active event sets of all supervisor's states. A useful direction is to use the active event set based criteria for PR of the supervisors to check the controllability property of the desired languages. Another useful direction is the use of the active event sets to facilitate the proof of the controllability and the nonblocking property. Regarding system modelling, the decomposition of the system to subsystems appears to facilitate fault modeling. Regarding fault modeling, it is important to mention that is a more complete modeling of the system, even if the faults are not detectable. The above direction is becoming more and more necessary in industry 4.0 manufacturing systems, not only because faults affect the productivity and safety of the system but also due to the strong correlation and common control strategies required for fault detection, fault tolerance control, and handling of cyber-attacks, indicatively see [19,20].

2. A DES Model of the Manufacturing Cell

2.1. Description of the Manufacturing Cell

The manufacturing cell studied here is the cell presented in [1,3,11]. The main components (see Figure 1), namely the subsystems, of the manufacturing cell, are a circular rotating table with four discrete positions, a classifier and transportation device, a drilling machine, a testing device, a robotic manipulator, and a feeding device. The feeding device receives raw products and delivers them to the classifier and transportation (C&T) device. There are three types of raw products, having variable dimensions, that can be transferred into the system. The C&T device classifies the raw products and either transfers them to the table or rejects them. A product is rejected if its dimensions are out of range. The raw products are drilled by the drilling machine and tested by the testing device. The testing device has two different types of processing. Testing process A is performed whenever a product has been successfully drilled. Testing process B is performed when there is a fault in the drilling process, e.g., tool break down. The products are retrieved from the table by the robotic manipulator. The retrieved products are stored by the manipulator to an appropriate storing magazine. There are three storing magazines. The first type of drilled products are stored to the first magazine. The second type are stored to the second magazine. The rejected drilled products are stored to the third magazine.

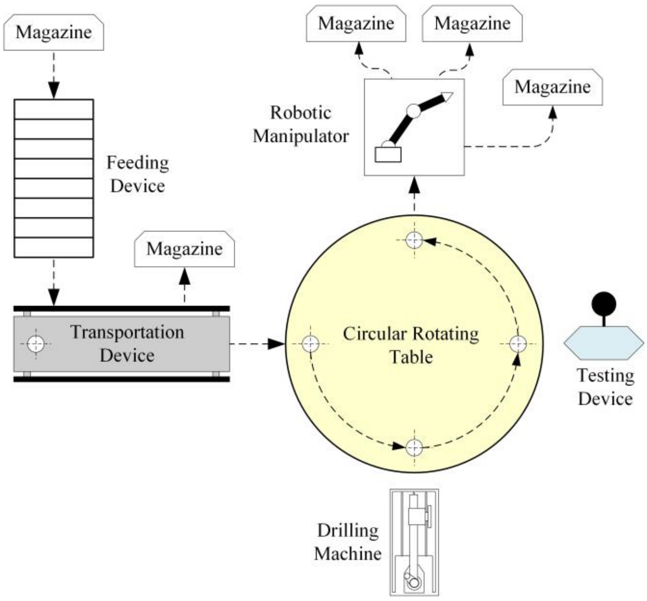

Figure 1. The manufacturing cell.

In [1,3,11], the subsystems of the manufacturing cell are presented without considering the presence of faults, except the drilling subsystem where the possibility of the presence of fault has been considered. Here, the possibility of the presence of faults, in all subsystems, is considered. Also here, each subsystem of the manufacturing cell with possible faults will be modelled, in the form of discrete event systems (DES) in the class of finite deterministic automata (see [21–23]), i.e., in six tuples of the form $\mathbf{G} = (\mathbb{Q}, \mathbb{E}, f, \mathbb{H}, x_0, \mathbb{Q}_m)$. $\mathbb{Q}$ denotes the set of the states of $\mathbf{G}$. $\mathbb{E}$ denotes the event set (alphabet) of $\mathbf{G}$. $\mathbb{H}$ denotes the map from each state of $\mathbf{G}$ to the respective set of active events. f denotes the transition function of $\mathbf{G}$.

x_0 denotes the initial state of $\mathbf{G}$. $\mathbb{Q}_m$ denotes the set of the marked states of $\mathbf{G}$. The closed and the marked behavior of $\mathbf{G}$ (see [10]) are denoted by $\mathbb{L}(\mathbf{G})$ and $\mathbb{L}_m(\mathbf{G})$, respectively. For the two behaviors of $\mathbf{G}$, it holds that $\mathbb{L}_m(\mathbf{G}) \subseteq \mathbb{L}(\mathbf{G}) \subseteq \mathbb{E}^*$, where $\mathbb{E}^*$ denotes the Kleene Star of $\mathbb{E}$, see [6,8]. The set of the uncontrollable events of each subsystem is denoted in the form: $\mathbb{E}_{uc} \subseteq \mathbb{E}$. According to [6,8], if $\overline{\mathbb{L}_m(\mathbf{G})} = \mathbb{L}(\mathbf{G})$ then $\mathbf{G}$ is a nonblocking automaton, where $\bar{\cdot}$ denotes the prefix closure of the argument language, see [6,8].

2.2. The Model of the Circular Rotating Table with Faults

The model of the circular rotating table in the presence of faults is developed here to be $\mathbf{G}_T = (\mathbb{Q}_T, \mathbb{E}_T, f_T, \mathbb{H}_T, x_{T,0}, \mathbb{Q}_{T,m})$. The set of the states is $\mathbb{Q}_T = \{q_{T,1}, q_{T,2}, q_{T,3}\}$. The initial state is $x_{T,0} = q_{T,1}$. The set of the marked states is $\mathbb{Q}_{T,m} = \{q_{T,1}\}$. The states of the circular rotating table are presented in Table 1. The rotating table is in faulty mode when the rotation mechanism is out of order or malfunctions as well as when the rotation is obstructed by obstacles in the workspace.

Table 1. States of the circular rotating table.

Symbol	State Description
$q_{T,1}$	The table is idle
$q_{T,2}$	The table is moving
$q_{T,3}$	The table is in faulty mode

The alphabet is $\mathbb{E}_T = \{e_{T,1}, e_{T,2}, e_{T,3}, e_{T,4}\}$. In Table 2, the events of the circular rotating table, are presented.

Table 2. Events of the circular rotating table.

Symbol	Event Description
$e_{T,1}$	The table starts rotating for 90^{o}
$e_{T,2}$	The table stops rotating
$e_{T,3}$	A fault took place
$e_{T,4}$	The fault has been repaired

The 1st event is a command signal. The 2nd event is a measurable signal. The 3rd event is observable, via an appropriate data acquisition and monitoring system, see [14–16]. Clearly, the 1st and the 4th event (repair signal) being produced by the Supervisory Control and Data Acquisition (SCADA) or a button pushed on by the supervising/maintenance personnel, are observable. The set of the controllable events is $\mathbb{E}_{T,c} = \{e_{T,1}, e_{T,4}\}$ and the set of the uncontrollable events is $\mathbb{E}_{T,uc} = \{e_{T,2}, e_{T,3}\}$. The sets of the active events are $\mathbb{H}_T(q_{T,1}) = \{e_{T,1}\}$, $\mathbb{H}_T(q_{T,2}) = \{e_{T,2}, e_{T,3}\}$ and $\mathbb{H}_T(q_{T,3}) = \{e_{T,4}\}$. The values of the transition functions are $f_T(q_{T,1}, e_{T,1}) = q_{T,2}$, $f_T(q_{T,2}, e_{T,2}) = q_{T,1}$, $f_T(q_{T,2}, e_{T,3}) = q_{T,3}$ and $f_T(q_{T,3}, e_{T,4}) = q_{T,1}$.

$\mathbf{G}_T$ is a nonblocking automaton, i.e., $\mathbb{L}(\mathbf{G}_T) = \overline{\mathbb{L}_m(\mathbf{G}_T)}$, where $\mathbb{L}_m(\mathbf{G}_T) = (e_{T,1}(e_{T,2} + e_{T,3}e_{T,4}))^*$. In Figure 2, the state diagram of $\mathbf{G}_T$ is presented. If the presence of faults is neglected, then the state diagram is reduced to that in, see [1,3,11].

2.3. The Model of the Classifier and Transportation Device with Faults

The model of the C&T device, in the presence of faults, is developed here to be $\mathbf{G}_C = (\mathbb{Q}_C, \mathbb{E}_C, f_C, \mathbb{H}_C, x_{C,0}, \mathbb{Q}_{C,m})$. The set of the states is $\mathbb{Q}_C = \{q_{C,1}, q_{C,2}, q_{C,3}, q_{C,4}, q_{C,5}\}$. The initial state is $x_{C,0} = q_{C,1}$. The set of the marked states is $\mathbb{Q}_{C,m} = \{q_{C,1}\}$. In Table 3, the states of the C&T device are presented. According to [11] the C&T device consist of two linear actuators, a capacitive sensor, an optic sensor, an inductive sensor and an appropriate sensor for the height measurement of the pieces. Regarding the linear actuator, the C&T

device is in faulty mode due to an excess of wear, a cracking, a backlash, lubricant related faults, etc., see [24]. Regarding the sensors, the C&T device is in faulty mode due to an external interference to the measurements, very common short-circuit faults, and common sensor drift, see [25].

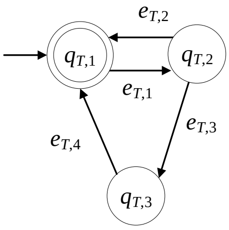

Figure 2. The state diagram of $\mathbf{G}_T$.

Table 3. States of the classifier and transportation device.

Symbol	State Description
$q_{C,1}$	The device is idle
$q_{C,2}$	The device is classifying
$q_{C,3}$	The device has been paused
$q_{C,4}$	The device is transporting
$q_{C,5}$	The device is in faulty mode

The alphabet is $\mathbb{E}_C = \{e_{C,1}, e_{C,2}, e_{C,3}, e_{C,4}, e_{C,5}, e_{C,6}, e_{C,7}\}$. In Table 4, the events of the C&T device are presented.

Table 4. Events of the classifier and transportation device.

Symbol	Event Description
$e_{C,1}$	The device starts classifying
$e_{C,2}$	The product has been classified and accepted
$e_{C,3}$	The product has been classified and rejected
$e_{C,4}$	The device starts transporting.
$e_{C,5}$	The product has been transported.
$e_{C,6}$	A fault took place at the device
$e_{C,7}$	A fault has been repaired at the device

The events $e_{C,1}$ and $e_{C,4}$ are command signals, and the events $e_{C,2}$, $e_{C,3}$, and $e_{C,5}$ are measurable signals. The event $e_{C,6}$ is observable through an appropriate monitoring system, see [14–16]. Clearly, the two command signals and the repair signal, being produced by the SCADA or a button pushed by the supervising/maintenance personnel, are observable. The controllable event set is $\mathbb{E}_{C,c} = \{e_{C,1}, e_{C,4}, e_{C,7}\}$ and the uncontrollable event set is $\mathbb{E}_{C,uc} = \{e_{C,2}, e_{C,3}, e_{C,5}, e_{C,6}\}$. The sets of the active events of $\mathbf{G}_C$ are

$$\mathbb{H}_C(q_{C,1}) = \{e_{C,1}\},\ \mathbb{H}_C(q_{C,2}) = \{e_{C,2}, e_{C,3}, e_{C,6}\},\ \mathbb{H}_C(q_{C,3}) = \{e_{C,4}, e_{C,6}\},$$
$$\mathbb{H}_C(q_{C,4}) = \{e_{C,5}, e_{C,6}\},\ \mathbb{H}_C(q_{C,5}) = \{e_{C,7}\}.$$

The values of the transition function of $\mathbf{G}_C$ are

$$f_C(q_{C,1}, e_{C,1}) = q_{C,2},\ f_C(q_{C,2}, e_{C,2}) = q_{C,3},\ f_C(q_{C,2}, e_{C,6}) = q_{C,5},\ f_C(q_{C,2}, e_{C,3}) = q_{C,1},$$
$$f_C(q_{C,3}, e_{C,4}) = q_{C,4},\ f_C(q_{C,3}, e_{C,6}) = q_{C,5},\ f_C(q_{C,4}, e_{C,5}) = q_{C,1},\ f_C(q_{C,4}, e_{C,6}) = q_{C,5},$$
$$f_C(q_{C,5}, e_{C,7}) = q_{C,1}.$$

$\mathbf{G}_C$ is a nonblocking automaton, i.e., $\overline{\mathbb{L}_m(\mathbf{G}_C)} = \mathbb{L}(\mathbf{G}_C)$, where

$$\mathbb{L}_m(\mathbf{G}_C) = (e_{C,1}(e_{C,3} + e_{C,6}e_{C,7} + e_{C,2}(e_{C,6}e_{C,7} + e_{C,4}(e_{C,5} + e_{C,6}e_{C,7}))))^*.$$

In Figure 3, the state diagram of $\mathbf{G}_C$ is presented. In the nonfaulty case, the diagram is reduced to that in [1,3,11].

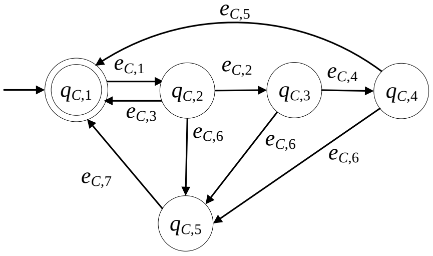

Figure 3. State diagram of $\mathbf{G}_C$.

2.4. *The Model of the Drilling Machine with Faults*

The model of the drilling machine, in the presence of faults, is expressed as $\mathbf{G}_D = (\mathbb{Q}_D, \mathbb{E}_D, f_D, \mathbb{H}_D, x_{D,0}, \mathbb{Q}_{D,m})$. The set of the states is $\mathbb{Q}_D = \{q_{D,1}, q_{D,2}, q_{D,3}\}$. The initial state is $x_{D,0} = q_{D,1}$. The set of the marked states is $\mathbb{Q}_{D,m} = \{q_{D,1}\}$. In Table 5, the states of the drilling machine are presented. The drilling machine is in faulty mode in cases of tool wear (see [26] and the references therein) or if the drilling tool is broken or one of the three linear actuators of the drilling machine is in faulty mode (see [11]), as well as if the drilling motor malfunctions, indicatively see [27,28]. The signals indicating the presence of such faults are derived through appropriate soft sensors that use the outputs of electric, speed and/or torque sensors, indicatively, see [26–28].

Table 5. States of the drilling machine.

Symbol	State Description
$q_{D,1}$	The drilling machine is idle
$q_{D,2}$	The drilling machine is working (drilling)
$q_{D,3}$	The drill is in faulty mode

The alphabet is $\mathbb{E}_D = \{e_{D,1}, e_{D,2}, e_{D,3}, e_{D,4}\}$. In Table 6, the events of the drilling machine are presented.

Table 6. Events of the drilling machine.

Symbol	Event Description
$e_{D,1}$	The drilling machine starts drilling.
$e_{D,2}$	Drilling has been successfully completed
$e_{D,3}$	The machine is in faulty mode
$e_{D,4}$	The machine has been repaired.

The 1st event is a command signal. The rest are appropriate observable signals. Thus, the set of the controllable events is $\mathbb{E}_{D,c} = \{e_{D,1}, e_{D,4}\}$ and the set of the uncontrollable events is $\mathbb{E}_{D,uc} = \{e_{D,2}, e_{D,3}\}$. The sets of the active events of $\mathbf{G}_D$, are $\mathbb{H}_D(q_{D,1}) = \{e_{D,1}\}$, $\mathbb{H}_D(q_{D,2}) = \{e_{D,2}, e_{D,3}\}$, $\mathbb{H}_D(q_{D,3}) = \{e_{D,4}\}$. The values of transition function are $f_D(q_{D,1}, e_{D,1}) = q_{D,2}$, $f_D(q_{D,2}, e_{D,2}) = q_{D,1}$, $f_D(q_{D,2}, e_{D,3}) = q_{D,3}$, $f_D(q_{D,3}, e_{D,4}) = q_{D,1}$.

Note that $\mathbf{G}_D$ is nonblocking, i.e., $\overline{\mathbb{L}_m(\mathbf{G}_D)} = \mathbb{L}(\mathbf{G}_D)$, where $\mathbb{L}_m(\mathbf{G}_D) = (e_{D,1}(e_{D,2} + e_{D,3}e_{D,4}))^*$.

In Figure 4, the state diagram of the automaton of the drilling machine is presented. This diagram has first been presented in [1,3,11].

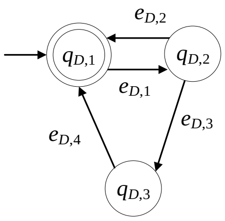

Figure 4. State diagram of $\mathbf{G}_D$.

2.5. The Model of the Testing Device with Faults

The model of the testing device, in the presence of faults, is developed to be of the six tuple form $\mathbf{G}_B = (\mathbb{Q}_B, \mathbb{E}_B, f_B, \mathbb{H}_B, x_{B,0}, \mathbb{Q}_{B,m})$. The set of the states is $\mathbb{Q}_B = \{q_{B,1}, q_{B,2}, q_{B,3}\}$. The initial state is $x_{B,0} = q_{B,1}$. The set of the marked states is $\mathbb{Q}_{B,m} = \{q_{B,1}\}$. In Table 7, the states of the testing device are presented. According to [11], the testing device consist of a linear actuator and a vacuum generator, as well as appropriate sensors. The testing device is in faulty mode for the reasons analogous to those presented for the C&T device, see also [24,25]. The repair signal can be produced in the same way to the previous subsystems and so is observable.

Table 7. States of the testing device.

Symbol	State Description
$q_{B,1}$	The testing device is idle
$q_{B,2}$	The testing device is working
$q_{B,3}$	The testing device is in faulty mode

The alphabet is $\mathbb{E}_B = \{e_{B,1}, e_{B,2}, e_{B,3}, e_{B,4}, e_{B,5}\}$. In Table 8, the events of the testing device are presented.

Table 8. Events of the testing device.

Symbol	State Description
$e_{B,1}$	The device begins the testing process *A*
$e_{B,2}$	The device begins the testing process *B*
$e_{B,3}$	The product is tested
$e_{B,4}$	A fault of the device took place
$e_{B,5}$	A fault of the device has been repaired

The 1st and the 2nd event are command signals. The rest are observable signals. Thus, the set of the controllable events is $\mathbb{E}_{B,c} = \{e_{B,1}, e_{B,2}, e_{B,5}\}$ and the set of the uncontrollable events is $\mathbb{E}_{B,uc} = \{e_{B,3}, e_{B,4}\}$. The sets of the active events of $\mathbf{G}_B$ are

$$\mathbb{H}_B(q_{B,1}) = \{e_{B,1}, e_{B,2}\},\ \mathbb{H}_B(q_{B,2}) = \{e_{B,3}, e_{B,4}\},\ \mathbb{H}_B(q_{B,3}) = \{e_{B,5}\}.$$

The values of the transition function are

$$f_B(q_{B,1}, e_{B,1}) = q_{B,2},\ f_B(q_{B,1}, e_{B,2}) = q_{B,2},\ f_B(q_{B,2}, e_{B,3}) = q_{B,1},\ f_B(q_{B,2}, e_{B,4}) = q_{B,3},$$
$$f_B(q_{B,3}, e_{B,5}) = q_{B,1}$$

The automaton $\mathbf{G}_B$ is nonblocking, i.e., $\overline{\mathbb{L}_m(\mathbf{G}_B)} = \mathbb{L}(\mathbf{G}_B)$, where

$$\mathbb{L}_m(\mathbf{G}_B) = ((e_{B,1} + e_{B,2})(e_{B,3} + e_{B,4}e_{B,5}))^*$$

In Figure 5, the state diagram of the automaton of the testing device is presented. In the nonfaulty case, the diagram is reduced to that in, see [1,3,11].

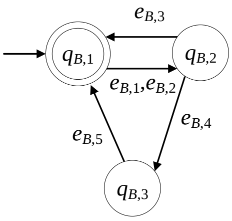

Figure 5. The state diagram of $\mathbf{G}_B$.

2.6. *The Model of the Robotic Manipulator with Faults*

The model of the robotic manipulator, in the presence of faults, is developed to be $\mathbf{G}_R = (\mathbb{Q}_R, \mathbb{E}_R, f_R, \mathbb{H}_R, x_{R,0}, \mathbb{Q}_{R,m})$. The set of the states is $\mathbb{Q}_R = \{q_{R,1}, q_{R,2}, q_{R,3}, q_{R,4}\}$. The initial state is $x_{R,0} = q_{R,1}$. The set of the marked states is $\mathbb{Q}_{R,m} = \{q_{R,1}\}$. In Table 9, the states of the robotic manipulator are presented. The robotic manipulator can be in faulty mode for various reasons, indicatively see [29–31].

Table 9. States of the robotic manipulator.

Symbol	State Description
$q_{R,1}$	The manipulator is idle
$q_{R,2}$	The manipulator is retrieving a product from the table
$q_{R,3}$	The manipulator is storing a product
$q_{R,4}$	The manipulator is in faulty mode

The alphabet is $\mathbb{E}_R = \{e_{R,1}, e_{R,2}, e_{R,3}, e_{R,4}, e_{R,5}\}$. In Table 10, the events of the robotic manipulator are presented.

Table 10. Events of the robotic manipulator.

Symbol	Event Description
$e_{R,1}$	The manipulator starts retrieving and storing a product.
$e_{R,2}$	The manipulator has retrieved a product from the table
$e_{R,3}$	The manipulator has stored a product
$e_{R,4}$	A fault of the manipulator took place
$e_{R,5}$	A fault of the manipulator has been repaired

The 1st event is a command signal. The rest are observable signals. The controllable events set is $\mathbb{E}_{R,c} = \{e_{R,1}, e_{R,5}\}$ and the set of the uncontrollable events is $\mathbb{E}_{R,uc} = \{e_{R,2}, e_{R,3}, e_{R,4}\}$. The sets of the active events of $\mathbf{G}_R$ are

$$\mathbb{H}_R(q_{R,1}) = \{e_{R,1}\},\ \mathbb{H}_R(q_{R,2}) = \{e_{R,2}, e_{R,4}\},\ \mathbb{H}_R(q_{R,3}) = \{e_{R,3}, e_{R,4}\},\\ \mathbb{H}_R(q_{R,4}) = \{e_{R,5}\}$$

The values of the transition function of $\mathbf{G}_R$ are

$$f_R(q_{R,1}, e_{R,1}) = q_{R,2},\ f_R(q_{R,2}, e_{R,2}) = q_{R,3},\ f_R(q_{R,2}, e_{R,4}) = q_{R,4},\ f_R(q_{R,3}, e_{R,3}) = q_{R,1},\\ f_R(q_{R,3}, e_{R,4}) = q_{R,4},\ f_R(q_{R,4}, e_{R,5}) = q_{R,1}$$

$\mathbf{G}_R$ is nonblocking automaton, i.e., $\overline{\mathbb{L}_m(\mathbf{G}_R)} = \mathbb{L}(\mathbf{G}_R)$, where

$$\mathbb{L}_m(\mathbf{G}_R) = (e_{R,1}(e_{R,4}e_{R,5} + e_{R,2}(e_{R,3} + e_{R,4}e_{R,5})))^*$$

In Figure 6, the state diagram of $\mathbf{G}_R$ is presented. In the nonfaulty case, the diagram is reduced to that in [1,3,11].

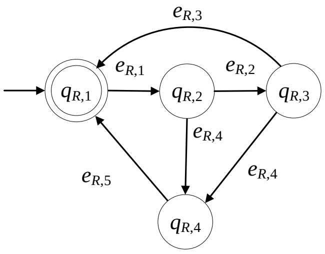

Figure 6. State diagram of $\mathbf{G}_R$.

2.7. The Model of the Feeding Device with Faults

The model of the feeding device in the presence of faults is developed to be $\mathbf{G}_F = (\mathbb{Q}_F, \mathbb{E}_F, f_F, \mathbb{H}_F, x_{F,0}, \mathbb{Q}_{F,m})$. The set of the states is $\mathbb{Q}_F = \{q_{F,1}, q_{F,2}, q_{F,3}, q_{F,4}\}$. The initial state is $x_{F,0} = q_{F,1}$. The set of the marked states is $\mathbb{Q}_{F,m} = \{q_{F,1}\}$. In Table 11 the description of the states of the feeding device are presented. According to [11] the feeding device consist of a linear actuator, a rotary actuator and appropriate sensors. The feeding device is in faulty mode for the same reasons to those presented for the C&T device, see [24,25,32]. The repair signal can be produced in the same way to the previous subsystems and so is observable.

Table 11. States of the feeding device.

Symbol	State Description
$q_{F,1}$	The device is idle
$q_{F,2}$	The device is working
$q_{F,3}$	The device is out of rough pieces
$q_{F,4}$	The device is in faulty mode

The alphabet is $\mathbb{E}_F = \{e_{F,1}, e_{F,2}, e_{F,3}, e_{F,4}, e_{F,5}, e_{F,6}\}$. In Table 12, the events of the feeding device are presented.

Table 12. Events of the feeding device.

Symbol	Event Description
$e_{F,1}$	The device starts working
$e_{F,2}$	A product has been fed
$e_{F,3}$	The device is out of rough products
$e_{F,4}$	The device has been refilled with rough products
$e_{F,5}$	A fault took place at the device.
$e_{F,6}$	A fault has been repaired at the device.

The event $e_{F,1}$ is a command signal and the events $e_{F,2}$, $e_{F,3}$, $e_{F,4}$, $e_{F,5}$ and $e_{F,6}$ are observable signals. Thus, the set of the controllable events is $\mathbb{E}_{F,c} = \{e_{F,1}, e_{F,6}\}$ and the set of the uncontrollable events is $\mathbb{E}_{F,uc} = \{e_{F,2}, e_{F,3}, e_{F,4}, e_{F,5}\}$. The sets of the active events of $\mathbf{G}_F$ are $\mathbb{H}_F(q_{F,1}) = \{e_{F,1}\}$, $\mathbb{H}_F(q_{F,3}) = \{e_{F,4}, e_{F,5}\}$, $\mathbb{H}_F(q_{F,4}) = \{e_{F,6}\}$. The values of the transition function are

$$f_F(q_{F,1}, e_{F,1}) = q_{F,2},\ f_F(q_{F,2}, e_{F,2}) = q_{F,1},\ f_F(q_{F,2}, e_{F,3}) = q_{F,3},$$
$$f_F(q_{F,2}, e_{F,5}) = q_{F,4},\ f_F(q_{F,3}, e_{F,4}) = q_{F,1},\ f_F(q_{F,3}, e_{F,5}) = q_{F,4},$$
$$f_F(q_{F,4}, e_{F,6}) = q_{F,1}$$

$\mathbf{G}_F$ is a nonblocking automaton i.e., $\overline{\mathbb{L}_m(\mathbf{G}_F)} = \mathbb{L}(\mathbf{G}_F)$, where

$$\mathbb{L}_m(\mathbf{G}_F) = (e_{F,1}(e_{F,2} + e_{F,5}e_{F,6} + e_{F,3}(e_{F,4} + e_{F,5}e_{F,6})))^*$$

In Figure 7, the state diagram of $\mathbf{G}_F$ is presented. In the nonfaulty case, the diagram is reduced to that in [1,3,11].

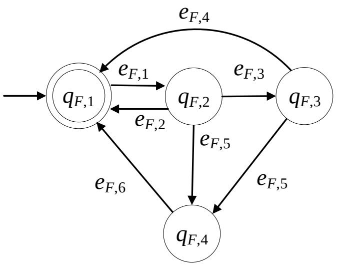

Figure 7. State diagram of $\mathbf{G}_F$.

2.8. The Cell Model as a Shuffle

Since the event sets of the subsystems presented in Section 2 are disjoint sets, the model $\mathbf{G}$ of the manufacturing cell can be expressed as the shuffle [6] of the of the subsystems and can be expressed in the synchronous product form $\mathbf{G} = \mathbf{G}_T||\mathbf{G}_C||\mathbf{G}_D||\mathbf{G}_B||\mathbf{G}_R||\mathbf{G}_F$. In [6,8], the definition and the properties of the synchronous product [6], or alternatively the parallel connection [8], are presented. The set of its states is $\mathbb{Q} = \mathbb{Q}_T \times \mathbb{Q}_C \times \mathbb{Q}_D \times \mathbb{Q}_B \times \mathbb{Q}_R \times \mathbb{Q}_F$ and the states are of the form $q = (q_T, q_C, q_D, q_B, q_R, q_F)$. The alphabet of $\mathbf{G}$ is $\mathbb{E} = \mathbb{E}_T \cup \mathbb{E}_C \cup \mathbb{E}_D \cup \mathbb{E}_B \cup \mathbb{E}_R \cup \mathbb{E}_F$. Clearly, all transitions of the subsystems are feasible. The active event sets of $\mathbf{G}$ satisfy the following property
$\mathbb{H}((q_T, q_C, q_D, q_B, q_R, q_F)) = \mathbb{H}_T(q_T) \cup \mathbb{H}_C(q_C) \cup \mathbb{H}_D(q_D) \cup \mathbb{H}_B(q_B) \cup \mathbb{H}_R(q_R) \cup \mathbb{H}_F(q_F)$
and the set of the marked states is $\mathbb{Q}_m = \{(q_{T,1}, q_{C,1}, q_{D,1}, q_{B,1}, q_{R,1}, q_{F,1})\}$.

3. Desired Languages

In [11], a set of safety and functionality specifications has been presented. Here, the above specifications are enriched with requirements considering the possibility of the presence of the faults. Note that in the faulty case of the drilling machine the product is tested to be accepted or rejected. Here, except the drilling machine, after the detection of a fault to another subsystem and its repair, the process of the subsystem will reinitiate to complete the task with respect to the current product.

In particular, the desired specifications, in the eventual presence of faults, are formulated, here, as follows:

1. When a fault takes place in the table or in the robotic manipulator, then the commands to leave from the idle state of the rest of the cell's systems are deactivated until the fault's repair.
2. The circular table is allowed to start rotating only if there is raw product in the appropriate position or a drilled piece in the drilling machine or a tested product in the testing device.
3. Table's rotation and raw product transportation to the cell do not take place simultaneously.
4. Table's rotation and drilling do not take place simultaneously.
5. Table's rotation and testing do not take place simultaneously.
6. Table's rotation and product retrieving, through the robotic manipulator, do not take place simultaneously.
7. The C&T device is not allowed to have two or more raw products in its output and the drilling machine is not allowed to start working without a product.
8. The drilling machine is not allowed to drill a product twice and the testing processes *A* and *B* of the testing device can begin only after the successful completion of the respective drilling process.

9. The robotic manipulator can retrieve a product only if there is a tested product in the respective position and the table's rotation cannot initiate with a non-retrieved piece in the respective position.

The goal of the above rules is to protect the system from undesirable and/or malicious situations such as the ones described in the Section 1. Some possible malfunctions that may take place, are prevented by the following measures, being imposed by the nine specification rules,

- *Measure* 1: Unnecessary rotations of the table are avoided, as rule 2 does not allow table rotation without a product in one of the predefined positions of the table.
- *Measure* 2: Undesirable cooperation between the table and a device is prevented from rules 3–6 allowing table rotation only when the respective device is in idle mode.
- *Measure* 3: The case of overflow in the output of the C&T device and the case of drilling with no product in the respective position, are prevented from Rule 7.
- *Measure* 4: Product loss, through second drilling and/or testing of an unfinished product, is prevented from rule 8.
- *Measure* 5: Rule 9 prevents the loss of finished products.

The 1st specification can be decomposed to two prefixed closed regular languages. The first regular language is for the table of the system, while the second regular language is for the robotic manipulator

$$
\begin{aligned}
{}^{1}\mathbb{K}_1 &= \overline{((e_{C,1}+e_{D,1}+e_{B,1}+e_{R,1}+e_{F,1}+e_{T,4})^* e_{T,3}(e_{T,3})^* e_{T,4})^*},\\
{}^{1}\mathbb{K}_2 &= \overline{((e_{T,1}+e_{C,1}+e_{D,1}+e_{B,1}+e_{F,1}+e_{R,5})^* e_{R,4}(e_{R,4})^* e_{R,5})^*}
\end{aligned}
$$

The 2nd specification is expressed by the following prefixed closed regular language:

$$
{}^{2}\mathbb{K} = \overline{((e_{C,5}+e_{D,2}+e_{D,3}+e_{B,3})(e_{C,5}+e_{D,2}+e_{D,3}+e_{B,3})^* e_{T,1})^*}
$$

The 3rd specification is expressed by the following prefixed closed regular language:

$$
{}^{3}\mathbb{K} = \overline{((e_{T,2}+e_{T,4}+e_{C,5}+e_{C,6})^*(e_{T,1}+e_{C,4})(e_{T,2}+e_{T,4}+e_{C,5}+e_{C,6}))^*}.
$$

The 4th specification is expressed by the following prefixed closed regular language:

$$
{}^{4}\mathbb{K} = \overline{((e_{T,2}+e_{T,4}+e_{D,2}+e_{D,4})^*(e_{T,1}+e_{D,1})(e_{T,2}+e_{T,4}+e_{D,2}+e_{D,4}))^*}.
$$

The 5th specification is expressed by the following prefixed closed regular language:

$$
{}^{5}\mathbb{K} = \overline{((e_{T,2}+e_{T,4}+e_{B,3}+e_{B,5})^*(e_{T,1}+e_{B,1}+e_{B,2})(e_{T,2}+e_{T,4}+e_{B,3}+e_{B,5}))^*}.
$$

The 6th specification is expressed by the following prefixed closed regular language:

$$
{}^{6}\mathbb{K} = \overline{((e_{T,2}+e_{T,4}+e_{R,2}+e_{R,5})^*(e_{T,1}+e_{R,1})(e_{T,2}+e_{T,4}+e_{R,2}+e_{R,5}))^*}
$$

The 7th specification is expressed by the following prefixed closed regular language:

$$
{}^{7}\mathbb{K} = \overline{\Big((e_{T,1}+e_{C,4})^* e_{C,5}(e_{C,5})^* e_{T,1}(e_{C,5})^*\big(e_{C,4}(e_{C,5})^*+\varepsilon\big)^* e_{D,1}\Big)^*}
$$

The 8th specification can be analyzed to the following two prefixed closed regular languages:

$$
{}^{8}\mathbb{K}_1 = \overline{((e_{D,1})^* e_{D,2}(e_{D,2})^* e_{B,1})^*}, {}^{8}\mathbb{K}_2 = \overline{((e_{D,1})^* e_{D,3}(e_{D,3})^* e_{B,2})^*}.
$$

The 9th specification is expressed by the following prefixed closed regular language

$$
{}^{9}\mathbb{K} = \overline{((e_{T,1})^* e_{B,3}(e_{B,3})^* e_{T,1}(e_{B,3})^* e_{R,1})^*}
$$

Using the same indices, the alphabets of the above prefixed closed regular languages are

$$
\begin{gathered}
{}^{1}\mathbb{E}_{S,1} = \{e_{C,1}, e_{D,1}, e_{B,1}, e_{R,1}, e_{F,1}, e_{T,3}, e_{T,4}\},\ {}^{1}\mathbb{E}_{S,2} = \{e_{T,1}, e_{C,1}, e_{D,1}, e_{B,1}, e_{F,1}, e_{R,4}, e_{R,5}\},\\
{}^{2}\mathbb{E}_{S} = \{e_{T,1}, e_{C,5}, e_{D,2}, e_{D,3}, e_{B,3}\}, {}^{3}\mathbb{E}_{S} = \{e_{T,1}, e_{T,2}, e_{T,4}, e_{C,4}, e_{C,5}, e_{C,6}\},\\
{}^{4}\mathbb{E}_{S} = \{e_{T,1}, e_{T,2}, e_{T,4}, e_{D,1}, e_{D,2}, e_{D,4}\},\ {}^{5}\mathbb{E}_{S} = \{e_{T,1}, e_{T,2}, e_{T,4}, e_{B,1}, e_{B,2}, e_{B,3}, e_{B,5}\},\\
{}^{6}\mathbb{E}_{S} = \{e_{T,1}, e_{T,2}, e_{T,4}, e_{R,1}, e_{R,2}, e_{R,5}\},\ {}^{7}\mathbb{E}_{S} = \{e_{T,1}, e_{C,4}, e_{C,5}, e_{D,1}\},\\
{}^{8}\mathbb{E}_{S,1} = \{e_{D,1}, e_{D,2}, e_{B,1}\},\ {}^{8}\mathbb{E}_{S,2} = \{e_{D,1}, e_{D,3}, e_{B,2}\},\ {}^{9}\mathbb{E}_{S} = \{e_{T,1}, e_{B,3}, e_{R,1}\}
\end{gathered}
$$

To satisfy the specifications 1–9, the automaton **G** will be controlled by appropriate supervisors. To this end, similarly to [18,33] and because the specifications are expressed by prefixed closed languages, the performance of the resulting controlled automaton is proposed to be described by the following 11 desired languages

$$ {}^{1}\mathbb{K}_{D,1} = {}^{1}P_{1}^{-1}\left(\overline{{}^{1}\mathbb{K}_{1}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{1}P_{1}^{-1}\left({}^{1}\mathbb{K}_{1}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{1} $$

$$ {}^{1}\mathbb{K}_{D,2} = {}^{1}P_{2}^{-1}\left(\overline{{}^{1}\mathbb{K}_{2}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{1}P_{2}^{-1}\left({}^{1}\mathbb{K}_{2}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{2} $$

$$ {}^{2}\mathbb{K}_{D} = {}^{2}P^{-1}\left(\overline{{}^{2}\mathbb{K}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{2}P^{-1}\left({}^{2}\mathbb{K}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{3} $$

$$ {}^{3}\mathbb{K}_{D} = {}^{3}P^{-1}\left(\overline{{}^{3}\mathbb{K}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{3}P^{-1}\left({}^{3}\mathbb{K}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{4} $$

$$ {}^{4}\mathbb{K}_{D} = {}^{4}P^{-1}\left(\overline{{}^{4}\mathbb{K}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{4}P^{-1}\left({}^{4}\mathbb{K}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{5} $$

$$ {}^{5}\mathbb{K}_{D} = {}^{5}P^{-1}\left(\overline{{}^{5}\mathbb{K}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{5}P^{-1}\left({}^{5}\mathbb{K}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{6} $$

$$ {}^{6}\mathbb{K}_{D} = {}^{6}P^{-1}\left(\overline{{}^{6}\mathbb{K}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{6}P^{-1}\left({}^{6}\mathbb{K}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{7} $$

$$ {}^{7}\mathbb{K}_{D} = {}^{7}P^{-1}\left(\overline{{}^{7}\mathbb{K}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{7}P^{-1}\left({}^{7}\mathbb{K}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{8} $$

$$ {}^{8}\mathbb{K}_{D,1} = {}^{8}P_{1}^{-1}\left(\overline{{}^{8}\mathbb{K}_{1}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{8}P_{1}^{-1}\left({}^{8}\mathbb{K}_{1}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{9} $$

$$ {}^{8}\mathbb{K}_{D,2} = {}^{8}P_{2}^{-1}\left(\overline{{}^{8}\mathbb{K}_{2}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{8}P_{2}^{-1}\left({}^{8}\mathbb{K}_{2}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{10} $$

$$ {}^{9}\mathbb{K}_{D} = {}^{9}P^{-1}\left(\overline{{}^{9}\mathbb{K}}\right) \cap \mathbb{L}_{m}(\mathbf{G}) = {}^{9}P^{-1}\left({}^{9}\mathbb{K}\right) \cap \mathbb{L}_{m}(\mathbf{G}) \tag{11} $$

where ${}^{1}P_{1}$ and ${}^{1}P_{2}$ denote the projections of $\mathbb{E}^{*}$ to ${}^{1}\mathbb{E}_{S,1}^{*}$ and ${}^{1}\mathbb{E}_{S,2}^{*}$, respectively. ${}^{8}P_{1}$ and ${}^{8}P_{2}$ denote the projections of $\mathbb{E}^{*}$ to ${}^{8}\mathbb{E}_{S,1}^{*}$ and ${}^{8}\mathbb{E}_{S,2}^{*}$, respectively. ${}^{2}P$ till ${}^{7}P$ denote the projections of $\mathbb{E}^{*}$ to ${}^{2}\mathbb{E}_{S}^{*}$ till ${}^{7}\mathbb{E}_{S}^{*}$, respectively. ${}^{9}P$ denotes the projection of $\mathbb{E}^{*}$ to ${}^{9}\mathbb{E}_{S}^{*}$.

4. Supervisors

4.1. Notation and Properties of Supervisory Design

In order to control an automaton, let **G**, a finite deterministic automaton, called supervisor and denoted by $\mathbf{S} = (\mathbb{Q}_{S}, \mathbb{E}_{S}, f_{S}, \mathbb{H}_{S}, x_{S,0}, \mathbb{Q}_{S,m})$, will be used. The closed and the marked behavior of the controlled automaton by the aforementioned supervisor are equal to the closed and the marked behavior of the synchronous product [6] (or parallel composition [8]) of **S** and **G**, denoted by $\mathbf{S}||\mathbf{G}$. The complexity of **S** (indicatively see [13,34]) is the triad including the number of the states, the number of the events and the number of the transitions of **S**.

The control action of **S** to **G** is physical realizable (PR) (see [35]) if the transitions of **G** due to its uncontrollable events are not disactivated by $\mathbf{S}||\mathbf{G}$. The performance of the controlled automaton is nonblocking if $\mathbf{S}||\mathbf{G}$ is a nonblocking automaton, see [6,8]. Here, the case of multiple supervisors in a modular scheme will be used. For more details about the modular supervisory design, see [6,8] and the extensions developed in [18–33].

4.2. A Two-State Supervisor form Realizing the First Six and The 8th Specifications

The automaton $\mathbf{S}_1 = (\mathbb{Q}_{S,1}, \mathbb{E}_{S,1}, f_{S,1}, \mathbb{H}_{S,1}, x_{S,1,0}, \mathbb{Q}_{S,1,m})$ denotes a class of supervisors. The cardinality of the set of the states of $\mathbf{S}_1$ is equal to 2, i.e., $\mathbb{Q}_{S,1} = \{q_{S,1,1}, q_{S,1,2}\}$. The class of supervisors depends upon four regular expressions, denoted by ${}^1c_1$, ${}^1c_2$, ${}^1c_3$ and ${}^1c_4$. For the definition and properties of regular expressions, see [6,8]. Their alphabets are denoted by ${}^1\mathbb{E}_{c,1}$, ${}^1\mathbb{E}_{c,2}$, ${}^1\mathbb{E}_{c,3}$ and ${}^1\mathbb{E}_{c,4}$, respectively. The alphabet of $\mathbf{S}_1$ is $\mathbb{E}_{S,1} = {}^1\mathbb{E}_{c,1} \cup {}^1\mathbb{E}_{c,2} \cup {}^1\mathbb{E}_{c,3} \cup {}^1\mathbb{E}_{c,4}$. The initial state of $\mathbf{S}_1$ is $x_{S,1,0} = q_{S,1,1}$. It is considered that all states are marked, i.e., $\mathbb{Q}_{S,1,m} = \mathbb{Q}_{S,1}$. The active event sets of $\mathbf{S}_1$ are $\mathbb{H}_{S,1}(q_{S,1,1}) = {}^1\mathbb{E}_{c,1} \cup {}^1\mathbb{E}_{c,2}$ and $\mathbb{H}_{S,1}(q_{S,1,2}) = {}^1\mathbb{E}_{c,3} \cup {}^1\mathbb{E}_{c,4}$. The values of the transition function of $\mathbf{S}_1$ are

$$f_{S,1}(q_{S,1,1}, e) = q_{S,1,1},\ \forall e \in {}^1\mathbb{E}_{c,1},\ f_{S,1}(q_{S,1,1}, e) = q_{S,1,2},\ \forall e \in {}^1\mathbb{E}_{c,2},$$
$$f_{S,1}(q_{S,1,2}, e) = q_{S,1,2},\ \forall e \in {}^1\mathbb{E}_{c,3},\ f_{S,1}(q_{S,1,2}, e) = q_{S,1,1},\ \forall e \in {}^1\mathbb{E}_{c,4}$$

The complexity triad of $\mathbf{S}_1$ is $(2,\ |\mathbb{E}_{S,1}|, |\mathbb{E}_{S,1}|)$, where $|\bullet|$ denotes the cardinality of the argument set. The state diagram of $\mathbf{S}_1$ is depicted in Figure 8.

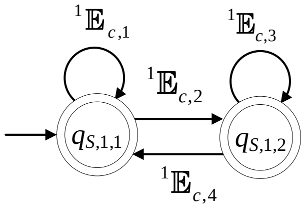

Figure 8. State diagram of $\mathbf{S}_1$.

$\mathbf{S}_1$ will be used for the realization of seven automata, where their closed and the marked behaviors will be equal to the prefixed closed regular languages ${}^1\mathbb{K}_1$, ${}^1\mathbb{K}_2$, ${}^2\mathbb{K}$, ${}^3\mathbb{K}$, ${}^4\mathbb{K}$,${}^5\mathbb{K}$ and ${}^6\mathbb{K}$, respectively. In Table 13, the supervisor's symbol derived, using $\mathbf{S}_1$, the respective languages and their complexity triad, are presented. According to Table 13, the alphabets of the regular expressions are uniquely determined. Indicatively, for ${}^1\mathbf{S}_{1,1}$ it holds that ${}^1\mathbb{E}_{c,1} = \{e_{C,1}, e_{D,1}, e_{B,1}, e_{R,1}, e_{F,1}\}$, ${}^1\mathbb{E}_{c,2} = {}^1\mathbb{E}_{c,3} = \{e_{T,3}\}$ and ${}^1\mathbb{E}_{c,4} = \{e_{T,4}\}$.

4.3. A Three-State Supervisor Realizing the 9th Specification

The supervisor automaton, realizing ${}^9\mathbb{K}$, is of the form $\mathbf{S}_2 = (\mathbb{Q}_{S,2}, \mathbb{E}_{S,2}, f_{S,2}, \mathbb{H}_{S,2}, x_{S,2,0}, \mathbb{Q}_{S,2,m})$. The set of the states of $\mathbf{S}_2$ is $\mathbb{Q}_{S,2} = \{q_{S,2,1}, q_{S,2,2}, q_{S,2,3}\}$ and $|\mathbb{Q}_{S,2}|= 3$. The alphabet of $\mathbf{S}_2$ is $\mathbb{E}_{S,2} = {}^9\mathbb{E}_S$. Its initial state is denoted by $x_{S,2,0} = q_{S,2,1}$. All states of $\mathbf{S}_2$ are marked, i.e., $\mathbb{Q}_{S,2,m} = \mathbb{Q}_{S,2}$. The sets of the active events, per state of $\mathbf{S}_2$, are $\mathbb{H}_{S,2}(q_{S,2,1}) = \{e_{T,1}, e_{B,3}\}$, $\mathbb{H}_{S,2}(q_{S,2,2}) = \{e_{T,1}, e_{B,3}\}$ and $\mathbb{H}_{S,2}(q_{S,2,3}) = \{e_{B,3}, e_{R,1}\}$. The values of the transition function of $\mathbf{S}_2$ are

$$f_{S,2}(q_{S,2,1}, e_{T,1}) = q_{S,2,1},\ f_{S,2}(q_{S,2,1}, e_{B,3}) = q_{S,2,2},\ f_{S,2}(q_{S,2,2}, e_{B,3}) = q_{S,2,2},$$
$$f_{S,2}(q_{S,2,2}, e_{T,1}) = q_{S,2,3},\ f_{S,2}(q_{S,2,3}, e_{B,3}) = q_{S,2,3},\ f_{S,2}(q_{S,2,3}, e_{R,1}) = q_{S,2,1}$$

The complexity triad of $\mathbf{S}_2$ is $(3,\ 3,\ 6)$. Its state diagram is presented in Figure 9.

4.4. A Four-State Supervisor Realizing the 7th Specification

The supervisor automaton, realizing ${}^7\mathbb{K}$, is of the form $\mathbf{S}_3 = (\mathbb{Q}_{S,3}, \mathbb{E}_{S,3}, f_{S,3}, \mathbb{H}_{S,3}, x_{S,3,0}, \mathbb{Q}_{S,3,m})$. The set of the states of $\mathbf{S}_3$ is $\mathbb{Q}_{S,3} = \{q_{S,3,1}, q_{S,3,2}, q_{S,3,3}, q_{S,3,4}\}$ and $|\mathbb{Q}_{S,3}|= 4$. The alphabet of $\mathbf{S}_3$ is $\mathbb{E}_{S,3} = {}^7\mathbb{E}_S$. Its initial state is denoted by $x_{S,3,0} = q_{S,3,1}$. All states of $\mathbf{S}_3$ are marked, i.e., $\mathbb{Q}_{S,3,m} = \mathbb{Q}_{S,3}$. The sets of the active events, per state of $\mathbf{S}_3$, are

$$\mathbb{H}_{S,3}(q_{S,3,1}) = \{e_{T,1}, e_{C,4}, e_{C,5}\},\ \mathbb{H}_{S,3}(q_{S,3,2}) = \{e_{T,1}, e_{C,5}\},\ \mathbb{H}_{S,3}(q_{S,3,3}) = \{e_{D,1}, e_{C,4}\}$$
$$\text{and } \mathbb{H}_{S,3}(q_{S,3,4}) = \{e_{D,1}, e_{C,5}\}$$

The values of the transition function of $\mathbf{S}_3$ are

$$\begin{gathered} f_{S,3}(q_{S,3,1}, e_{T,1}) = q_{S,3,1},\ f_{S,3}(q_{S,3,1}, e_{C,4}) = q_{S,3,1},\ f_{S,3}(q_{S,3,1}, e_{C,5}) = q_{S,3,2}, \\ f_{S,3}(q_{S,3,2}, e_{C,5}) = q_{S,3,2},\ f_{S,3}(q_{S,3,2}, e_{T,1}) = q_{S,3,3},\ f_{S,3}(q_{S,3,3}, e_{C,5}) = q_{S,3,3}, \\ f_{S,3}(q_{S,3,3}, e_{D,1}) = q_{S,3,1},\ f_{S,3}(q_{S,3,3}, e_{C,4}) = q_{S,3,4},\ f_{S,3}(q_{S,3,4}, e_{C,5}) = q_{S,3,4}, \\ f_{S,3}(q_{S,3,4}, e_{D,1}) = q_{S,3,1} \end{gathered}$$

The complexity triad of $\mathbf{S}_3$ is $(4,\ 4,\ 10)$. Its state diagram is presented in Figure 10.

Table 13. Supervisors derived by $\mathbf{S}_1$.

Supervisor	Behavior	Regular Expressions	Complexity
${}^1\mathbf{S}_{1,1}$	${}^1\mathbb{K}_1$	${}^1c_1 = e_{C,1} + e_{D,1} + e_{B,1} + e_{R,1} + e_{F,1} + e_{T,4}$, ${}^1c_2 = {}^1c_3 = e_{T,3}, {}^1c_4 = e_{T,4}$	(2, 7, 9)
${}^1\mathbf{S}_{1,2}$	${}^1\mathbb{K}_2$	${}^1c_1 = e_{T,1} + e_{C,1} + e_{D,1} + e_{B,1} + e_{F,1} + e_{R,5}$, ${}^1c_2 = {}^1c_3 = e_{R,4}, {}^1c_4 = e_{R,5}$	(2, 7, 9)
${}^2\mathbf{S}_1$	${}^2\mathbb{K}$	${}^1c_1 = \varepsilon, {}^1c_2 = {}^1c_3 = e_{C,5} + e_{D,2} + e_{D,3} + e_{B,3},\ {}^1c_4 = e_{T,1}$	(2, 5, 9)
${}^3\mathbf{S}_1$	${}^3\mathbb{K}$	${}^1c_1 = e_{T,2} + e_{T,4} + e_{C,5} + e_{C,6}$, ${}^1c_2 = e_{T,1} + e_{C,4}, {}^1c_3 = \varepsilon, {}^1c_4 = {}^1c_1$	(2, 6, 10)
${}^4\mathbf{S}_1$	${}^4\mathbb{K}$	${}^1c_1 = e_{T,2} + e_{T,4} + e_{D,2} + e_{D,4},\ {}^1c_2 = e_{T,1} + e_{D,1}$, ${}^1c_3 = \varepsilon, {}^1c_4 = {}^1c_1.$	(2, 6, 13)
${}^5\mathbf{S}_1$	${}^5\mathbb{K}$	${}^1c_1 = e_{T,2} + e_{T,4} + e_{B,3} + e_{B,5},\ {}^1c_2 = e_{T,1} + e_{B,1} + e_{B,2}$, ${}^1c_3 = \varepsilon, {}^1c_4 = {}^1c_1$	(2, 7, 11)
${}^6\mathbf{S}_1$	${}^6\mathbb{K}$	${}^1c_1 = e_{T,2} + e_{T,4} + e_{R,2} + e_{R,5}, {}^1c_2 = e_{T,1} + e_{R,1}$, ${}^1c_3 = \varepsilon, {}^1c_4 = {}^1c_1$	(2, 6, 12)
${}^8\mathbf{S}_{1,1}$	${}^8\mathbb{K}_1$	${}^1c_1 = e_{D,1},\ {}^1c_2 = {}^1c_3 = e_{D,2}, {}^1c_4 = e_{B,1}$	(2, 3, 4)
${}^8\mathbf{S}_{1,2}$	${}^8\mathbb{K}_2$	${}^1c_1 = e_{D,1},\ {}^1c_2 = {}^1c_3 = e_{D,3}, {}^1c_4 = e_{B,2}$	(2, 3, 4)

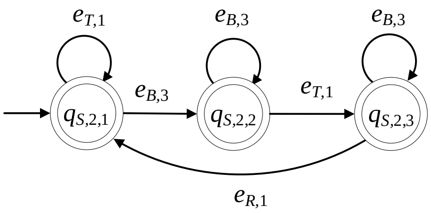

Figure 9. State diagram of $\mathbf{S}_2$.

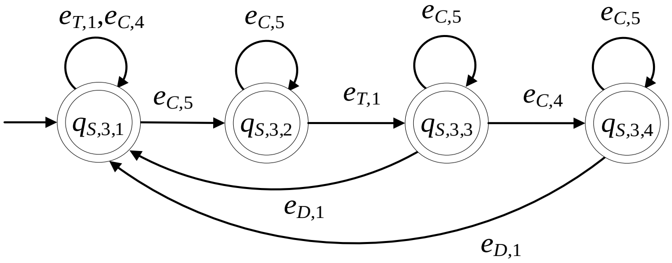

Figure 10. State diagram of $\mathbf{S}_3$.

5. The Performance of the Controlled Automaton

The supervisors proposed in Section 4, are interconnected to the automaton $\mathbf{G}$ of the manufacturing cell through the following multi argument synchronous product

$$\mathbf{G}_c = {}^1\mathbf{S}_{1,1}\Big|\Big|{}^1\mathbf{S}_{1,2}\Big|\Big|{}^2\mathbf{S}_1\Big|\Big|{}^3\mathbf{S}_1\Big|\Big|{}^4\mathbf{S}_1\Big|\Big|{}^5\mathbf{S}_1\Big|\Big|{}^6\mathbf{S}_1\Big|\Big|{}^8\mathbf{S}_{1,1}\Big|\Big|{}^8\mathbf{S}_{1,2}\Big|\Big|\mathbf{S}_2\Big|\Big|\mathbf{S}_3\Big|\Big|\mathbf{G}. \tag{12}$$

Automaton $\mathbf{G}_c$ is the controlled automaton. In this section, the performance of the controlled automaton $\mathbf{G}_c$ will be investigated. It will be proven that $\mathbf{G}_c$ satisfies the desired specifications 1–9, presented in Section 3. To this end and using the properties of the multi argument synchronous product (see [9,10]) and the property that the closed and the marked behaviors of the supervisors, are equal to the prefixed closed regular languages ${}^1\mathbb{K}_1$, ${}^1\mathbb{K}_2$, ${}^2\mathbb{K}$, ${}^3\mathbb{K}$, ${}^4\mathbb{K}$, ${}^5\mathbb{K}$, ${}^6\mathbb{K}$, ${}^7\mathbb{K}$, ${}^8\mathbb{K}_1$, and ${}^9\mathbb{K}$, respectively, the closed behavior and the marked behavior of $\mathbf{G}_c$ will first be computed

$$\begin{gathered}\mathbb{L}(\mathbf{G}_c) = \mathbb{L}(\mathbf{G}) \cap \left[\cap_{\lambda=2}^{7} {}^{\lambda}P^{-1}\left(\overline{{}^{\lambda}\mathbb{K}}\right)\right] \cap {}^1P_1^{-1}\left(\overline{{}^1\mathbb{K}_1}\right) \cap \\ \cap {}^1P_2^{-1}\left(\overline{{}^1\mathbb{K}_2}\right) \cap {}^8P_1^{-1}\left(\overline{{}^8\mathbb{K}_1}\right) \cap {}^8P_2^{-1}\left(\overline{{}^8\mathbb{K}_2}\right) \cap {}^9P^{-1}\left(\overline{{}^9\mathbb{K}}\right)\end{gathered} \tag{13}$$

$$\begin{gathered}\mathbb{L}_m(\mathbf{G}_c) = \mathbb{L}_m(\mathbf{G}) \cap [\cap_{\lambda=2}^{7} {}^{\lambda}P^{-1}({}^{\lambda}\mathbb{K})] \cap {}^1P_1^{-1}({}^1\mathbb{K}_1) \cap \\ \cap {}^1P_2^{-1}({}^1\mathbb{K}_2) \cap {}^8P_1^{-1}({}^8\mathbb{K}_1) \cap {}^8P_2^{-1}({}^8\mathbb{K}_2) \cap {}^9P^{-1}({}^9\mathbb{K}) = \\ = {}^1\mathbb{K}_{D,1} \cap {}^2\mathbb{K}_{D,1} \cap [\cap_{\lambda=2}^{7} {}^{\lambda}\mathbb{K}_D] \cap {}^8\mathbb{K}_{D,1} \cap {}^8\mathbb{K}_{D,2} \cap {}^9\mathbb{K}_D\end{gathered} \tag{14}$$

From (14), it is observed that the performance of the controlled automaton $\mathbf{G}_c$, regarding its marked behavior, is satisfactory. Regarding the closed behavior of $\mathbf{G}_c$, it is mentioned that in order to be satisfactory it is necessary and sufficient that $\mathbf{G}_c$ is nonblocking, i.e., $\overline{\mathbb{L}_m(\mathbf{G}_c)} = \mathbb{L}(\mathbf{G}_c)$. This property will be proven in Proposition 2.

In Figure 11, the operational flow of the present modular supervisory scheme is presented. The symbols $\mathbf{S}_1$ to $\mathbf{S}_{11}$ represent the eleven supervisors of the present control scheme (see Section 4). All commands (controllable events) are generated by the Generator/Scheduler and inputted to the eleven supervisors. All sensors' signals (uncontrollable events) are produced by the sensors and inputted to the eleven supervisors. The indications of faults (uncontrollable events) are produced by Fault Detectors. The outputs of all supervisors are connected to an "AND" block. An event is outputted by this block only if it is outputted by all eleven supervisors. The above algorithm is the main idea of modular supervising control.

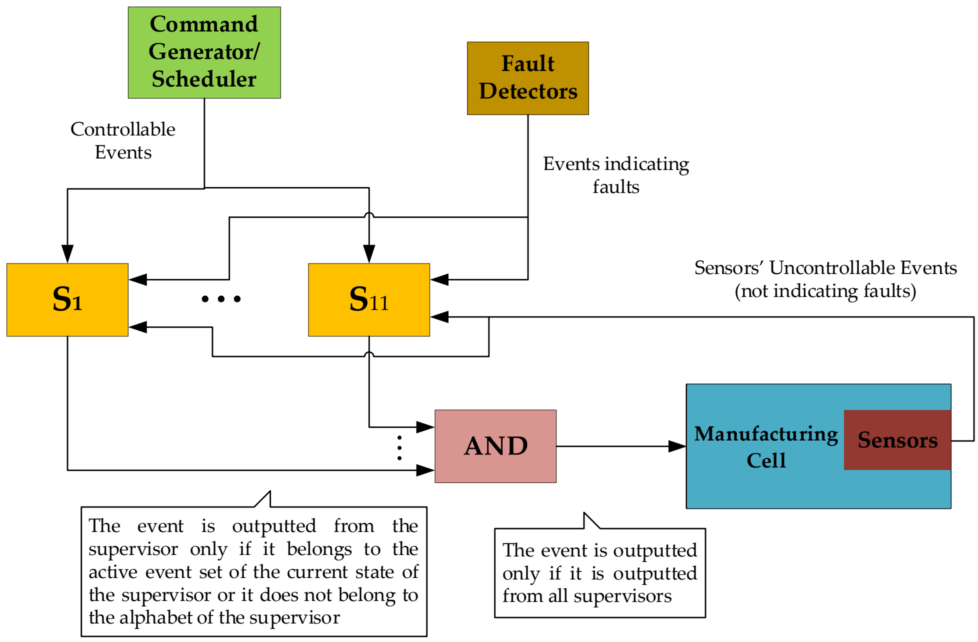
Command Generator/ Scheduler
Fault Detectors
Controllable Events
Events indicating faults
Sensors' Uncontrollable Events (not indicating faults)
S1
• • •
S11
AND
Manufacturing Cell
Sensors
The event is outputted from the supervisor only if it belongs to the active event set of the current state of the supervisor or it does not belong to the alphabet of the supervisor
The event is outputted only if it is outputted from all supervisors

Figure 11. Operational flow chart of the supervisory control scheme.

Before examining the closed behavior of the controlled automaton, it is necessary to examine the physical realizability (PR) of the synchronous product in Relation (12). The physical realizability (see [35,36]) is translated into the condition that the transitions of $\mathbf{G}$, activated by uncontrollable events, must not obstructed by the twelve supervisors.

Proposition 1: *The synchronous product of the designed supervisor scheme is PR, with respect to* $\mathbf{G}$*, through (12).*

Proof of Proposition 1: It holds that ${}^1\mathbb{H}_{S,1,1}({}^1q_{S,1,1}) \cap {}^1\mathbb{E}_{S,1,uc} = {}^1\mathbb{E}_{S,1,uc}$, where ${}^1\mathbb{E}_{S,1,uc} = {}^1\mathbb{E}_{S,1} \cap \mathbb{E}_{uc}$, and ${}^1\mathbb{E}_{S,1} \subset \mathbb{E}$. Using Corollary 1 in [35], it is concluded that ${}^1\mathbf{S}_{1,1}$ is PR with respect to $\mathbf{G}$, through ${}^1\mathbf{S}_{1,1}||\mathbf{G}$. The alphabet and the set of the uncontrollable events of ${}^1\mathbf{S}_{1,1}||\mathbf{G}$ are equal to the respective sets of $\mathbf{G}$. Also, it holds that ${}^1\mathbb{H}_{S,2}({}^1q_{S,1,2}) \cap {}^1\mathbb{E}_{S,2,uc} = {}^1\mathbb{E}_{S,2,uc}$ and ${}^1\mathbb{E}_{S,2} \subset \mathbb{E}$, where ${}^1\mathbb{E}_{S,2,uc} = {}^1\mathbb{E}_{S,2} \cap \mathbb{E}_{uc}$. Hence, using Corollary 1 of [32], it is concluded that ${}^1\mathbf{S}_{1,2}$ is PR with respect to ${}^1\mathbf{S}_{1,1}||\mathbf{G}$, through ${}^1\mathbf{S}_{1,2}||{}^1\mathbf{S}_{1,1}||\mathbf{G}$. It holds that ${}^i\mathbb{H}_{S,1}({}^iq_{S,1,1}) \cap {}^i\mathbb{E}_{S,uc} = {}^i\mathbb{E}_{S,uc}$, where ${}^i\mathbb{E}_{S,uc} = {}^i\mathbb{E}_S \cap \mathbb{E}_{uc}$ and $i \in \{2,\ldots,6\}$, as well as that ${}^i\mathbb{E}_S \subset \mathbb{E}$. The alphabet and the set of the uncontrollable events of $\left(\overset{i-1}{\underset{\lambda=2}{||}} {}^\lambda\mathbf{S}_1\right)||{}^1\mathbf{S}_{1,2}||{}^1\mathbf{S}_{1,1}||\mathbf{G}$ are equal to the respective sets of $\mathbf{G}$. Hence, using Corollary 1 of [32], it is concluded that ${}^i\mathbf{S}_1$ is PR, with respect to $\left(\overset{i-1}{\underset{\lambda=2}{||}} {}^\lambda\mathbf{S}_1\right)||{}^1\mathbf{S}_{1,2}||{}^1\mathbf{S}_{1,1}||\mathbf{G}$, through ${}^i\mathbf{S}_1||\left(\overset{i-1}{\underset{\lambda=2}{||}} {}^\lambda\mathbf{S}_1\right)||{}^1\mathbf{S}_{1,2}||{}^1\mathbf{S}_{1,1}||\mathbf{G}$. The alphabet and the set of the uncontrollable events of $\left(\overset{6}{\underset{\lambda=2}{||}} {}^\lambda\mathbf{S}_1\right)||{}^1\mathbf{S}_{1,2}||{}^1\mathbf{S}_{1,1}||\mathbf{G}$ are equal to the respective sets of $\mathbf{G}$. It holds that ${}^8\mathbb{E}_{S,1} \subset \mathbb{E}$, ${}^8\mathbb{H}_{S,1,1}({}^8q_{S,1,1}) \cap {}^8\mathbb{E}_{S,1,uc} = {}^8\mathbb{E}_{S,1,uc}$, where ${}^8\mathbb{E}_{S,1,uc} = {}^8\mathbb{E}_{S,1} \cap \mathbb{E}_{uc}$. Hence, using Corollary 1 of [32], it is concluded that ${}^8\mathbf{S}_{1,1}$ is PR, with respect to $\left(\overset{6}{\underset{\lambda=2}{||}} {}^\lambda\mathbf{S}_1\right)||{}^1\mathbf{S}_{1,2}||{}^1\mathbf{S}_{1,1}||\mathbf{G}$, through ${}^8\mathbf{S}_1||\left(\overset{6}{\underset{\lambda=2}{||}} ({}^\lambda\mathbf{S}_1)\right)||{}^1\mathbf{S}_{1,2}||{}^1\mathbf{S}_{1,1}||\mathbf{G}$. The alphabet and the set of the uncontrollable events of

${}^{8}\mathbf{S}_1||\left(\mathop{||}\limits_{\lambda=2}^{6}({}^{\lambda}\mathbf{S}_1)\right)||{}^{1}\mathbf{S}_{1,2}||{}^{1}\mathbf{S}_{1,1}||\mathbf{G}$ are equal to the respective sets of $\mathbf{G}$. Clearly, it holds that ${}^{8}\mathbb{E}_{S,2} \subset \mathbb{E}$, ${}^{8}\mathbb{H}_{S,1,2}({}^{8}q_{S,1,2}) \cap {}^{8}\mathbb{E}_{S,2,uc} = {}^{8}\mathbb{E}_{S,2,uc}$, where ${}^{8}\mathbb{E}_{S,2,uc} = {}^{8}\mathbb{E}_{S,2} \cap \mathbb{E}_{uc}$. Thus, using Corollary 1 of [35], it is concluded that ${}^{8}\mathbf{S}_{1,2}$ is PR, with respect to ${}^{8}\mathbf{S}_1||\left(\mathop{||}\limits_{\lambda=2}^{6}({}^{\lambda}\mathbf{S}_1)\right)||{}^{1}\mathbf{S}_{1,2}||{}^{1}\mathbf{S}_{1,1}||\mathbf{G}$, through ${}^{8}\mathbf{S}_{1,2}||{}^{8}\mathbf{S}_{1,1}||\left(\mathop{||}\limits_{\lambda=2}^{6}{}^{\lambda}\mathbf{S}_1\right)||{}^{1}\mathbf{S}_{1,2}||{}^{1}\mathbf{S}_{1,1}||\mathbf{G}$. The alphabet and the set of the uncontrollable events of ${}^{8}\mathbf{S}_{1,2}||{}^{8}\mathbf{S}_{1,1}||\left(\mathop{||}\limits_{\lambda=2}^{6}{}^{\lambda}\mathbf{S}_1\right)||{}^{1}\mathbf{S}_{1,2}||{}^{1}\mathbf{S}_{1,1}||\mathbf{G}$ are equal to the respective sets of $\mathbf{G}$. Also, it holds that $\mathbb{E}_{S,2} \subset \mathbb{E}$, $\mathbb{H}_{S,2}(q_{S,2}) \cap \mathbb{E}_{S,2,uc} = \mathbb{E}_{S,2,uc}$, where $\mathbb{E}_{S,2,uc} = \mathbb{E}_{S,2} \cap \mathbb{E}_{uc}$. Thus, using Corollary 1 of [32], it is concluded that $\mathbf{S}_2$ is PR with respect to

$${}^{8}\mathbf{S}_{1,2}||{}^{8}\mathbf{S}_{1,1}||\left(\mathop{||}\limits_{\lambda=2}^{6}{}^{\lambda}\mathbf{S}_1\right)||{}^{1}\mathbf{S}_{1,2}||{}^{1}\mathbf{S}_{1,1}||\mathbf{G},$$

through $\mathbf{S}_2||{}^{8}\mathbf{S}_{1,2}||{}^{8}\mathbf{S}_{1,1}||\left(\mathop{||}\limits_{\lambda=2}^{6}{}^{\lambda}\mathbf{S}_1\right)||{}^{1}\mathbf{S}_{1,2}||{}^{1}\mathbf{S}_{1,1}||\mathbf{G}$. Finally, the alphabet and the set of the uncontrollable events of $\mathbf{S}_2||{}^{8}\mathbf{S}_{1,2}||{}^{8}\mathbf{S}_{1,1}||\left(\mathop{||}\limits_{\lambda=2}^{6}{}^{\lambda}\mathbf{S}_1\right)||{}^{1}\mathbf{S}_{1,2}||{}^{1}\mathbf{S}_{1,1}||\mathbf{G}$ are equal to the respective sets of $\mathbf{G}$. Also, it holds that $\mathbb{E}_{S,3} \subset \mathbb{E}$, $\mathbb{H}_{S,3}(q_{S,3}) \cap \mathbb{E}_{S,3,uc} = \mathbb{E}_{S,3,uc}$, where $\mathbb{E}_{S,3,uc} = \mathbb{E}_{S,3} \cap \mathbb{E}_{uc}$. Hence, using Corollary 1 of [32], it is concluded that $\mathbf{S}_3$ is PR, with respect to

$$\mathbf{S}_2||{}^{8}\mathbf{S}_{1,2}||{}^{8}\mathbf{S}_{1,1}||\left(\mathop{||}\limits_{\lambda=2}^{6}{}^{\lambda}\mathbf{S}_1\right)||{}^{1}\mathbf{S}_{1,2}||{}^{1}\mathbf{S}_{1,1}||\mathbf{G},$$

through $\mathbf{S}_3||\mathbf{S}_2||{}^{8}\mathbf{S}_{1,2}||{}^{8}\mathbf{S}_{1,1}||\left(\mathop{||}\limits_{\lambda=2}^{6}{}^{\lambda}\mathbf{S}_1\right)||{}^{1}\mathbf{S}_{1,2}||{}^{1}\mathbf{S}_{1,1}||\mathbf{G}$. □

Proposition 2: *The controlled automaton $\mathbf{G}_c$ is a nonblocking automaton.*

Proof of Proposition 2: Next, the six automata of the corresponding subsystems under the influence of the twelve supervisors will be examined regarding the nonblocking property. It is important to mention that all supervisors are physical realizable regarding $\mathbf{G}$, i.e., all desired languages are controllable regarding $\mathbf{G}$. In what follows, it will be investigated if there are direct (single step) or indirect (more than one steps) transitions from the non-marked states of $\mathbf{G}_c$ to marked states of $\mathbf{G}_c$. Since all states of the supervisors are marked, all non-marked states of $\mathbf{G}_c$ include as a component at least one non-marked state of the subsystems of $\mathbf{G}$. To this end, for all non-marked states of each subsystem of $\mathbf{G}$, it will be investigated if there is a direct or indirect transition, not obstructed by the supervisor and the rest subsystems, that moves the subsystem to a marked state. Since $\mathbf{G}$ is the shuffle of its subsystems, this transition will not be related to any transition of the rest subsystems of $\mathbf{G}$. Thus, the aforementioned investigation will form a procedure, where upon checking one subsystem of $\mathbf{G}$, after the appropriate transition, the number of the non-marked state components of a non-marked state of $\mathbf{G}_c$ will be decreased by one. So, at the end of the procedure $\mathbf{G}_c$ will arrive at a marked state and the proof will be completed.

Starting the investigation with $\mathbf{G}_T$, it is observed that it has two non-marked states, namely, the states $q_{T,2}$ and $q_{T,3}$. Regarding $q_{T,2}$, it is recalled that $\mathbb{H}_T(q_{T,2}) = \mathbb{E}_{T,uc} = \{e_{T,2}, e_{T,3}\}$, $f_T(q_{T,2}, e_{T,2}) = q_{T,1}$. Since all supervisors are physical realizable, with respect to $\mathbf{G}$, it is observed that they are also PR, with respect to $\mathbf{G}_T$. Using this observation and the property that $\mathbf{G}$ is a shuffle, it is concluded that the transition from $q_{T,2}$ to the marked state $q_{T,1}$, is always feasible using the uncontrollable event $e_{T,2}$. Regarding $q_{T,3}$, it holds that $\mathbb{H}_T(q_{T,3}) = \{e_{T,4}\}$ and $f_T(q_{T,3}, e_{T,4}) = q_{T,1}$. It is observed that only the supervisors

${}^{1}\mathbf{S}_{1,1}$,${}^{3}\mathbf{S}_{1}$,${}^{4}\mathbf{S}_{1}$,${}^{5}\mathbf{S}_{1}$ and ${}^{6}\mathbf{S}_{1}$ have the event $e_{T,4}$ in their alphabet and that the event $e_{T,4}$ is in the active event sets of all supervisors' states. Hence, the transition from $q_{T,3}$ to the marked state $q_{T,1}$, using $e_{T,4}$ is not obstructed by the afore mentioned supervisors as well as the rest supervisors as they do not include $e_{T,4}$ in their alphabets. Also, recall that this transition is not obstructed by the rest subsystems, i.e., $\mathbf{G}_C$, $\mathbf{G}_D$, $\mathbf{G}_B$, $\mathbf{G}_R$ and $\mathbf{G}_F$, as their alphabets are disjoint sets with respect to $\mathbb{E}_T$. Hence, the transition from any state of $\mathbf{G}_c$, including as a component a non-marked state of $\mathbf{G}_T$, to a state of $\mathbf{G}_c$, where the non-marked state of $\mathbf{G}_T$ has been substituted by a marked state of $\mathbf{G}_T$, is always feasible.

The investigation will continue with $\mathbf{G}_C$. The automaton $\mathbf{G}_C$ has four non-marked states, namely the states $q_{C,2}$, $q_{C,3}$, $q_{C,4}$ and $q_{C,5}$. The repair event $e_{C,7}$ does not belong to any supervisor alphabet. Thus, the transition from the non-marked state $q_{C,5}$ to the marked state $q_{C,1}$ is always active, as $f_C(q_{C,5}, e_{C,7}) = q_{C,1}$. Regarding $q_{C,2}$ and $q_{C,4}$, it holds that $\mathbb{H}_C(q_{C,2}) = \{e_{C,3}\}$, $f_C(q_{C,2}, e_{C,3}) = q_{C,1}$, $\mathbb{H}_C(q_{C,4}) = \{e_{C,5}\}$, $f_C(q_{C,4}, e_{C,5}) = q_{C,1}$; $e_{C,3}, e_{C,5} \in \mathbb{E}_{C,uc}$. Hence, taking into account the physical realizability of the proposed supervisory scheme regarding $\mathbf{G}$ and the property that $\mathbf{G}$ is a shuffle, the transition from $q_{C,2}$ and $q_{C,4}$ to the marked state $q_{C,1}$ is always feasible using uncontrollable events. Finally, regarding $q_{C,3}$ it holds that $\mathbb{H}_C(q_{C,3}) = \{e_{C,4}, e_{C,6}\}$ and $f_C(q_{C,3}, e_{C,4}) = q_{C,4}$. It is observed that only the supervisors ${}^{3}\mathbf{S}_1$ and ${}^{7}\mathbf{S}_1$ have the event $e_{C,4}$ in their alphabet. Regarding ${}^{3}\mathbf{S}_1$, it is observed that in the first state the event $e_{C,4}$ is active. In the second state, the event $e_{C,4}$ is not active but there is always an active transition to the first state using an uncontrollable event. Thus, ${}^{3}\mathbf{S}_1$ does not obstruct the transition from $q_{C,3}$ to $q_{C,4}$. Regarding ${}^{7}\mathbf{S}_1$, it is observed that in the first and third state, the event $e_{C,4}$ is active. In the second and fourth state the event $e_{C,4}$ is not active but there is always an active transition to the third and first state using uncontrollable events. Thus, ${}^{7}\mathbf{S}_1$ does not obstruct the transition from $q_{C,3}$ to $q_{C,4}$. Also, the rest supervisors, namely all supervisors except ${}^{3}\mathbf{S}_1$ and ${}^{7}\mathbf{S}_1$ do not obstruct this transition, as they do not include $e_{C,4}$ in their alphabets. Regarding the automata $\mathbf{G}_T$, $\mathbf{G}_D$, $\mathbf{G}_B$, $\mathbf{G}_R$ and $\mathbf{G}_F$, their alphabets are disjoint sets with respect to $\mathbb{E}_C$. Hence, the transition from any state of $\mathbf{G}_c$ including as a component a non-marked state of $\mathbf{G}_C$, to a state of $\mathbf{G}_c$ where the non-marked state of $\mathbf{G}_C$ has been substituted by a marked state of $\mathbf{G}_C$, is always feasible.

The automaton $\mathbf{G}_D$ has two non-marked states, namely the states $q_{D,2}$ and $q_{D,3}$. Regarding $q_{D,2}$, it is recalled that $\mathbb{H}_D(q_{D,2}) = \mathbb{E}_{D,uc}$, $f_D(q_{D,2}, e_{D,2}) = q_{D,1}$. Since all supervisors are physical realizable with respect to $\mathbf{G}_D$, the transition from $q_{D,2}$ to the marked state $q_{D,1}$, using the uncontrollable event $q_{D,2}$ is always feasible. Finally, regarding, $q_{D,3}$ it holds that $\mathbb{H}_D(q_{D,3}) = \{e_{D,4}\}$ and $f_D(q_{D,3}, e_{D,4}) = q_{D,1}$. It is observed that only the supervisor ${}^{4}\mathbf{S}_1$ has the event $e_{D,4}$ in its alphabet. The event $e_{D,4}$ is active in all states of ${}^{4}\mathbf{S}_1$. Hence, the transition from $q_{D,3}$ to the marked state $q_{D,1}$, using $e_{D,4}$, is not obstructed by ${}^{4}\mathbf{S}_1$. Obviously, it is also not obstructed by the rest of the subsystems $\mathbf{G}_T$, $\mathbf{G}_C$, $\mathbf{G}_B$, $\mathbf{G}_R$ and $\mathbf{G}_F$, as their alphabets are disjoint sets with respect to $\mathbb{E}_D$. Hence, the transition from any state of $\mathbf{G}_c$, including as a component a non-marked state of $\mathbf{G}_D$, to a state of $\mathbf{G}_c$, where the non-marked state of $\mathbf{G}_D$ has been substituted by a marked state of $\mathbf{G}_D$, is always feasible.

The automaton $\mathbf{G}_B$ has also two non-marked states, namely the states $q_{B,2}$ and $q_{B,3}$. Regarding $q_{B,2}$, it is recalled that $\mathbb{H}_B(q_{B,2}) = \mathbb{E}_{B,uc}$, $f_B(q_{B,2}, e_{B,3}) = q_{B,1}$. Since all supervisors are physical realizable, with respect to $\mathbf{G}_B$, the transition from $q_{B,2}$ to the marked state $q_{B,1}$ is always feasible using the uncontrollable event $e_{B,3}$. Finally, regarding $q_{B,3}$, it holds that $\mathbb{H}_B(q_{B,3}) = \{e_{B,5}\}$ and $f_B(q_{B,3}, e_{B,5}) = q_{B,1}$. It is observed that only the supervisor ${}^{5}\mathbf{S}_1$ has the event $e_{B,5}$ in its alphabet. The event $e_{B,5}$ is active for all states of ${}^{5}\mathbf{S}_1$. Hence, the transition from $q_{B,3}$ to the marked state $q_{B,1}$, using $e_{B,5}$, is not obstructed by ${}^{5}\mathbf{S}_1$. Obviously, this transition is not obstructed by the rest of the subsystems $\mathbf{G}_T$, $\mathbf{G}_C$, $\mathbf{G}_D$, $\mathbf{G}_R$ and $\mathbf{G}_F$, as their alphabets are disjoint sets with respect to $\mathbb{E}_B$. Hence, the transition from any state of $\mathbf{G}_c$, including as a component a non-marked state of $\mathbf{G}_B$, to a state of $\mathbf{G}_c$, where the non-marked state of $\mathbf{G}_B$ has been substituted by a marked state of $\mathbf{G}_B$, is always feasible.

The automaton $\mathbf{G}_R$ has three non-marked states, namely the states $q_{R,2}$, $q_{R,3}$ and $q_{R,4}$. Regarding $q_{R,2}$ and $q_{R,3}$, it holds that $\mathbb{H}_R(q_{R,2}) = \{e_{R,2}, e_{R,4}\}$, $f_R(q_{R,2}, e_{R,2}) = q_{R,3}$,

$\mathbb{H}_R(q_{R,3}) = \{e_{R,3}, e_{R,4}\}$, $f_R(q_{R,3}, e_{R,3}) = q_{R,1}$, where $e_{R,2}, e_{R,3} \in \mathbb{E}_{R,uc}$. Hence, taking into account the physical realizability of the proposed supervisory scheme, with respect to $\mathbf{G}$, and the property that $\mathbf{G}$ is a shuffle, it is observed that the transitions from $q_{R,2}$ and $q_{R,3}$ to the marked state $q_{R,1}$ are always feasible using uncontrollable events. Finally, regarding $q_{R,4}$, it holds that $\mathbb{H}_R(q_{R,4}) = \{e_{R,5}\}$ and $f_R(q_{R,4}, e_{R,5}) = q_{R,1}$. It is observed that only the supervisors ${}^1\mathbf{S}_{1,2}$ and ${}^6\mathbf{S}_1$ have the event $e_{R,5}$ in their alphabet. The event $e_{R,5}$ belongs the active event sets of all states of these two supervisors. Hence, the transition from $q_{R,4}$ to the marked state $q_{R,1}$, using $e_{R,5}$, is not obstructed by ${}^1\mathbf{S}_{1,2}$ and ${}^6\mathbf{S}_1$ as well as the rest supervisors as they do not include $e_{R,5}$ in their alphabets. Also, this transition is not obstructed by the rest of the subsystems, namely $\mathbf{G}_T$, $\mathbf{G}_C$, $\mathbf{G}_D$, $\mathbf{G}_B$ and $\mathbf{G}_F$, as their alphabets are disjoint sets with respect to $\mathbb{E}_R$. Hence, the transition from any state of $\mathbf{G}_c$, including as a component a non-marked state of $\mathbf{G}_R$, to a state of $\mathbf{G}_c$, where the non-marked state of $\mathbf{G}_R$ has been substituted by a marked state of $\mathbf{G}_R$, is always feasible. Thus, the automaton $\mathbf{G}_{R,c}$ is a nonblocking automaton. □

Remark 1: *The nonblocking property of $\mathbf{G}_c$ is guaranteed regardless the consideration of faults in the subsystems, in the sense that the transitions from states of $\mathbf{G}_c$, being non-faulty and non-marked, to marked states of $\mathbf{G}_c$ are feasible without necessarily passing through faulty states.*

Remark 2: *The complexity of the proposed modular supervisor scheme is* $(25, 57, 101)$.

Remark 3: *The design of the first six supervisors and the 8-th supervisor are realized by a common parametric function block. The above characteristic contributes to the controller implementation facilitating the respective programming.*

6. The Case without Faults

In the case where there are no faults in the system, the models of the subsystems automata presented in Section 2, are reduced to appropriate sub-automata, denoted by $\tilde{\mathbf{G}}_T$, $\tilde{\mathbf{G}}_C$, $\tilde{\mathbf{G}}_D$, $\tilde{\mathbf{G}}_B$, $\tilde{\mathbf{G}}_R$ and $\tilde{\mathbf{G}}_F$. The above automata are derived by removing the faulty states, the events of the faults and the fault repair events as well as any transition related to the above states and events of the respective automata presented in Section 2. Also, in the no faults case, the desired languages presented in Section 3, are reduced to a set of new languages, denoted by ${}^1\tilde{\mathbb{K}}_1$, ${}^1\tilde{\mathbb{K}}_2$, ${}^2\tilde{\mathbb{K}}$, ${}^3\tilde{\mathbb{K}}$, ${}^4\tilde{\mathbb{K}}$, ${}^5\tilde{\mathbb{K}}$, ${}^6\tilde{\mathbb{K}}$, ${}^7\tilde{\mathbb{K}}$, ${}^8\tilde{\mathbb{K}}_1$, ${}^8\tilde{\mathbb{K}}_2$ and ${}^9\tilde{\mathbb{K}}$. The above languages are derived by the respective languages of the faulty case, upon substituting the events of faults and the fault repair events with the empty word ε. Finally, the supervisors realizing these new languages, ${}^1\tilde{\mathbf{S}}_{1,1}$, ${}^1\tilde{\mathbf{S}}_{1,2}$, ${}^2\tilde{\mathbf{S}}_1$, ${}^3\tilde{\mathbf{S}}_1$, ${}^4\tilde{\mathbf{S}}_1$, ${}^5\tilde{\mathbf{S}}_1$, ${}^6\tilde{\mathbf{S}}_1$, ${}^8\tilde{\mathbf{S}}_{1,1}$, ${}^8\tilde{\mathbf{S}}_{1,2}$, $\tilde{\mathbf{S}}_2$ and $\tilde{\mathbf{S}}_3$. The above supervisors are derived by the respective supervisors of the faulty case, upon removing the events of the faults and the fault repair events as well as the transitions, related only to these events, and finally upon removing the non-accessible states. It is important to mention that the supervisors ${}^1\tilde{\mathbf{S}}_{1,1}$ and ${}^1\tilde{\mathbf{S}}_{1,2}$, handle the faults of the table and the faults of the robotic manipulator, will now be single state automata with self-transitions triggered by all events in the alphabet of each supervisor. Hence, in the case without faults, the above two supervisors do not contribute to the performance of the control system and so they can be neglected.

In concluding, in the case without faults, the proposed here supervisory scheme is still effective.

7. Supervisor Implementation

An interesting issue, on the implementation of a supervisor control scheme, is the transition from event-based supervisors, built in the form of automata models, to standard signal-based PLC's operation, see [1,3,11]. To demonstrate the ease implementation of the proposed, here, supervisory control scheme, in real time industrial controllers such as

PLCs, PACs etc., the present supervisors are implemented in the international standard IEC 61131–3 (2013). Industry 4.0 trends for real time industrial controller implementation, can be found in [33] and the references therein. Also, details regarding programming for the implementation of supervisor automata can be found in [1,5] and the refences therein.

In Figures 12–14, the supervisors realized in Section 4, are implemented using the IEC 61131-3 (2013) Ladder Diagrams. The implementation, through Ladder Diagrams, has been preferred, as the Ladder Diagrams provide a good overview and are offered for engineer inspection. Figures 12–14, illustrate the ease implementability of the realized supervisors. As already mentioned in Section 4, the supervisors realized in the class of supervisors determined by $\mathbf{S}_1$, are also offered for implementation in the event-driven architecture of the IEC 61499 function blocks.

Regarding communication protocols, it is important to mention that the modern communication standard OPC UA as well as the Modbus protocol, being the typical PLC communication protocol, can be used through simple parametrization of the declared variables and the parameters of the default timers and the alarms of the PLC, see also [37]. Regarding further trends, imposed by Industry 4.0, see [33,37–39]. Finally, regarding the robotic manipulator, it is mentioned that the supervisor of the manipulator, implemented in PLC (see Figure 12), is interconnected to the robotic operations system (ROS2) following the directions presented in [40], providing an efficient framework.

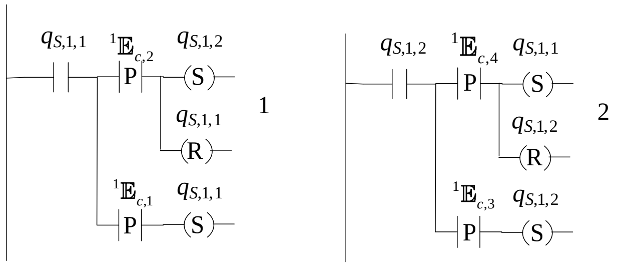

Figure 12. State diagram of $\mathbf{S}_1$.

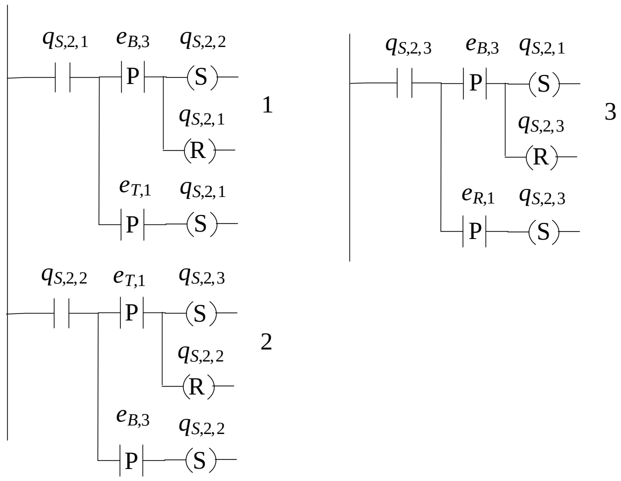

Figure 13. State diagram of $\mathbf{S}_2$.

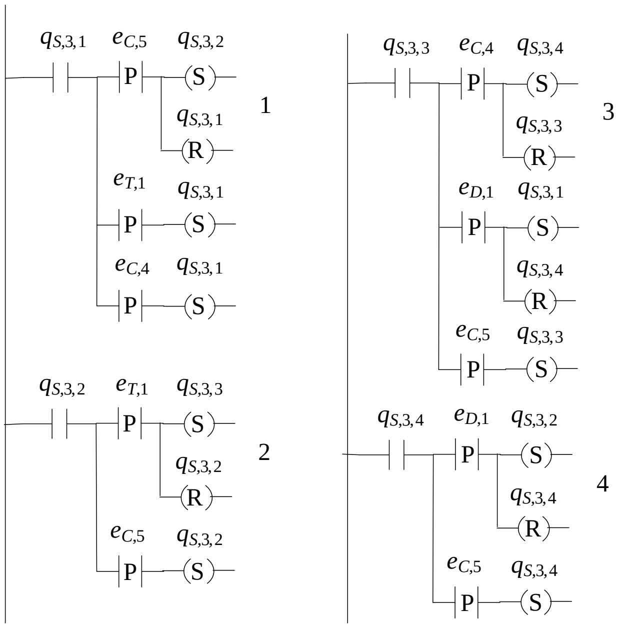

Figure 14. State diagram of $\mathbf{S}_3$.

8. Conclusions

In the present paper the model of manufacturing cell, in the presence of faults, has been developed through appropriate models of its subsystems. The DES models of all the system's components have been presented considering possible actuator/sensor faults. The total automaton of the manufacturing cell has also been presented. The desired behavior of the manufacturing cell has firstly been presented analytically, in the form of nine desired specifications. The desired specifications have been translated to appropriate eleven prefixed closed regular languages. The desired languages have been determined from the eleven regular languages in combination to the marked behavior of the total system. The regular languages have been realized by a set of eleven supervisors. The supervisors have been developed upon realizing a two-state class of automata and two other automata. The supervisors have been designed to be as possible maximally permissive without losing necessary performance properties, while guaranteeing PR regarding the total automaton of the manufacturing cell. The performance of the controlled automaton has been proven to have satisfactory closed behavior and marked behavior. The controllability of the eleven proposed languages and the nonblocking property of the controlled automaton have been proven. The complexity of the proposed supervisory scheme has been computed. Finally, implementability issues to modern industrial control devices have been figured out and the ladder diagrams of the three automata classes have been developed.

The feasibility of the results of the paper lies on two directions. The first direction is that the present supervisory control design is developed for a well-established and fully experimentally tested manufacturing cell with several applications, indicatively see [1,3,11]. The second is the implementation of the proposed supervisor scheme using Ladder diagrams (see Section 7).

The extension of the present supervisory control scheme, achieving tolerance to upper-level faults of a manufacturing process, to the case of partially observable lower-level faults in the devices of the process is currently under investigation.

Author Contributions: Conceptualization, N.D.K., F.N.K. and D.G.F.; Methodology, F.N.K. and D.G.F.; Validation, N.D.K. and F.N.K.; Investigation, D.G.F. and A.S.; Resources, N.D.K. and D.G.F.; Data curation, D.G.F. and A.S.; Writing—original draft preparation, N.D.K., F.N.K. and D.G.F.; Writing—review and editing, D.G.F. and A.S.; Supervision, N.D.K. and F.N.K.; Project administration, N.D.K., F.N.K. and D.G.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors would like to thank the anonymous reviewers for their fruitful comments.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations and Nomenclature

The capital bold letter $\mathbf{G}$, with appropriate indices, is used to denote manufacturing subsystems in DES form. The capital bold letter $\mathbf{S}$, with appropriate indices, is used to denote supervisor automata in DES form. Finally, the capital letter $\mathbb{K}$, with appropriate indices, is used to denote regular languages. In the following table, the acronyms used in the present paper are presented.
Acronyms

DES	Discrete Event System
SCT	Supervisory Control Theory
FMS	Flexible Manufacturing System
CNC	Computer Numerical Control
PLC	Programmable Logic Controller
IEC	International Electrotechnical Commission
C&T	Classifier and Transportation
SCADA	Supervisory Control and Data Acquisition
PR	Physical Realizability

A list including the symbols, used in the paper, is presented in the following table.
List of symbols.

$\mathbf{G}_{\phi}$	The automaton of the subsystem indexed by ϕ, where ϕ is considered to be an appropriate capital letter representing the subsystem
$\mathbb{Q}_{\phi}$, $q_{\phi,j}$	The set of states of $\mathbf{G}_{\phi}$, the j-th state of $\mathbf{G}_{\phi}$
$\mathbb{E}_{\phi}$, $\mathbb{E}_{\phi,uc}$, $e_{\phi,j}$	The alphabet of $\mathbf{G}_{\phi}$, the uncontrollable events set of $\mathbf{G}_{\phi}$, the j-th event of $\mathbf{G}_{\phi}$
$\mathbb{H}_{\phi}(q)$, f_{ϕ}	The active event set of the state q of $\mathbf{G}_{\phi}$, the transition function of $\mathbf{G}_{\phi}$
$x_{\phi,0}$, $\mathbb{Q}_{\phi,m}$	The initial state of $\mathbf{G}_{\phi}$, the set of the marked states of $\mathbf{G}_{\phi}$
$\mathbb{L}(\mathbf{G}_{\phi})$, $\mathbb{L}_m(\mathbf{G}_{\phi})$	The closed and the marked behavior of $\mathbf{G}_{\phi}$
$\mathbf{G}$, $\mathbf{G}_c$	The total automaton, the total controlled automaton
${}^{v}\mathbb{K}$, ${}^{v}\mathbb{K}_D$	The regular language of the v-th specification and the respective desired language
${}^{i}\mathbb{K}_j$, ${}^{i}\mathbb{K}_{D,j}$	The j-th regular language of the i-th specification and the respective desired language
${}^{i}\mathbb{E}_{S,j}$, ${}^{v}\mathbb{E}_S$,	The alphabet of ${}^{i}\mathbb{K}_j$, the alphabet of ${}^{v}\mathbb{K}$
${}^{i}\mathbb{E}_{S,j,uc}$, ${}^{v}\mathbb{E}_{S,uc}$	The uncontrollable event subsets of ${}^{i}\mathbb{E}_{S,j}$ and ${}^{v}\mathbb{E}_S$, respectively.
${}^{i}P_j$, ${}^{v}P$	The projections of $\mathbb{E}^*$ to ${}^{i}\mathbb{E}^*_{S,j}$ and ${}^{v}\mathbb{E}^*_S$, respectively.
${}^{i}\mathbf{S}_{1,j}$, ${}^{v}\mathbf{S}_1$	The supervisor automaton of the j-th regular language of the i specification, the supervisor automaton of the v-th specification
${}^{i}\mathbb{Q}_{S,1,j}$, ${}^{v}\mathbb{Q}_{S,1}$	The set of states of ${}^{i}\mathbf{S}_{1,j}$, the set of states of ${}^{v}\mathbf{S}_1$
${}^{i}q_{S,1,j,k}$, ${}^{v}q_{S,1,k}$	The k-th state of ${}^{i}\mathbf{S}_{1,j}$, the k-th state of ${}^{v}\mathbf{S}_1$
${}^{i}\mathbb{H}_{S,1,j}(q)$, ${}^{v}\mathbb{H}_{S,1}(q)$	The active event set of the state q of ${}^{i}\mathbf{S}_{1,j}$ and ${}^{v}\mathbf{S}_1$, respectively
${}^{i}f_{S,1,j}(q,e), {}^{v}f_{S,1}(q,e)$	The transition functions of ${}^{i}\mathbf{S}_{1,j}$ and ${}^{v}\mathbf{S}_1$, respectively
${}^{i}x_{S,1,j,0}$, ${}^{v}x_{S,1,0}$	The initial state of ${}^{i}\mathbf{S}_{1,j}$ and ${}^{v}\mathbf{S}_1$, respectively
${}^{i}\mathbb{Q}_{S,1,j,m}$, ${}^{v}\mathbb{Q}_{S,1,m}$	The set of the marked states of ${}^{i}\mathbf{S}_{1,j}$, the set of the marked states of ${}^{v}\mathbf{S}_1$

$\mathbf{S}_\lambda$	The supervisor automaton of ${}^{9}\mathbb{K}$ for $\lambda = 2$ and of ${}^{7}\mathbb{K}$ for $\lambda = 3$
$\mathbb{Q}_{S,\lambda}$, $q_{S,\lambda,j}$	The set of states of $\mathbf{S}_\lambda$, the j-th state of $\mathbf{S}_\lambda$
$\mathbb{H}_{S,\lambda}(q)$, $f_{S,\lambda}(q,e)$	The active event set of the state q of $\mathbf{S}_\lambda$, the transition function of $\mathbf{S}_\lambda$
$x_{S,\lambda,0}$, ${}^{i}\mathbb{Q}_{S,\lambda,m}$	The initial state of $\mathbf{S}_\lambda$, the set of the marked states of $\mathbf{S}_\lambda$

References

1. 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 Trans. Control Syst. Technol.* **2017**, *25*, 175–191. [CrossRef]
2. Pichard, R.; Philippot, A.; Saddem, R.; Riera, B. Safety of Manufacturing Systems Controllers by Logical Constraints with Safety Filter. *IEEE Trans. Control Syst. Technol.* **2019**, *27*, 1659–1667. [CrossRef]
3. de Queiroz, M.H.; Cury, J.E.R. Synthesis and implementation of local modular supervisory control for a manufacturing cell. In Proceedings of the 6th International Workshop in Discrete Event System, Zaragoza, Spain, 4 October 2002; pp. 377–382. [CrossRef]
4. Szpak, R.; de Queiroz, M.H.; Cury, J.E.R. Synthesis and implementation of supervisory control for manufacturing systems under processing uncertainties and time constraints. *IFAC Pap.* **2020**, *53*, 229–234. [CrossRef]
5. Prenzel, L.; Provost, J. PLC Implementation of Symbolic, Modular Supervisory Controllers. *IFAC Pap.* **2018**, *51*, 304–309. [CrossRef]
6. Wonham, W.M.; Kai, C. *Supervisory Control of Discrete-Event Systems*; Springer: Cham, Switzerland, 2019. [CrossRef]
7. Theis, J.; Mokhtarian, I.; Darabi, H. Process Mining of Programmable Logic Controllers: Input/Output Event Logs. In Proceedings of the 2019 IEEE 15th International Conference on Automation Science and Engineering (CASE), Vancouver, BC, Canada, 19 September 2019; pp. 216–221. [CrossRef]
8. Cassandras, C.G.; Lafortune, S. *Introduction to Discrete Event Systems*, 3rd ed.; Springer: Cham, Switzerland, 2021. [CrossRef]
9. Alves, M.V.S.; da Cunha, A.E.C.; Kawakami Carvalho, L.; Moreira, M.V.; Basilio, J.C. Robust supervisory control of discrete event systems against intermittent loss of observations. *Int. J. Control* **2021**, *94*, 1–13. [CrossRef]
10. Blanke, M.; Kinnaert, M.; Lunze, J.; Staroswiecki, M.; Schroder, J. *Diagnosis and Fault-Tolerant Control*, 3rd ed.; Springer: Berlin, Germany, 2016. [CrossRef]
11. Vieira, A.D.; Santos, E.A.P. Implementing PLC Supervisory Control of a Modular Production System with PLCs of Siemens and Rockwell Automation. Available online: http://www.biblioteca.pucpr.br/pergamum/biblioteca/img.php?arquivo=/000053/000053b4.pdf (accessed on 22 December 2022).
12. Lafortune, S.; Lin, F.; Hadjicostis, C.N. On the history of diagnosability and opacity in discrete event systems. *Annu. Rev. Control* **2018**, *45*, 257–266. [CrossRef]
13. Zaytoon, J.; Lafortune, S. Overview of fault diagnosis methods for discrete event systems. *Annu. Rev. Control* **2013**, *37*, 308–320. [CrossRef]
14. Cabral, F.G.; Moreira, M.V. Synchronous Diagnosis of Discrete-Event Systems. *IEEE Trans. Autom. Sci. Eng.* **2020**, *17*, 921–932. [CrossRef]
15. Hu, Y.; Ma, Z.; Li, Z. Design of Supervisors for Active Diagnosis in Discrete Event Systems. *IEEE Trans. Autom. Control* **2020**, *65*, 5159–5172. [CrossRef]
16. Wang, D.; Wang, X.; Li, Z. State-based fault diagnosis of discrete-event systems with partially observable outputs. *Inf. Sci.* **2020**, *529*, 87–100. [CrossRef]
17. Watanabe, A.T.Y.; Leal, A.B.; Cury, J.E.R.; de Queiroz, M.H. Combining Online Diagnosis and Prognosis for Safe Controllability. *IEEE Trans. Autom. Control* **2022**, *67*, 5563–5569. [CrossRef]
18. Watanabe, A.T.Y.; Sebem, R.; Leal, A.B.; Hounsell, M.d.S. Fault prognosis of discrete event systems: An overview. *Annu. Rev. Control* **2021**, *51*, 100–110. [CrossRef]
19. Yao, J.; Yin, X.; Li, S. On Attack Mitigation in Supervisory Control Systems: A Tolerant Control Approach. In Proceedings of the 2020 59th IEEE Conference on Decision and Control (CDC), Jeju Island, Republic of Korea, 14–18 December 2020. [CrossRef]
20. Cao, L.; Jiang, X.; Zhao, Y.; Wang, S.; You, D.; Xu, X. A Survey of Network Attacks on Cyber-Physical Systems. *IEEE Access* **2020**, *8*, 44219–44227. [CrossRef]
21. Koumboulis, F.N.; Fragkoulis, D.G.; Menexis, A.N. Supervisory Control for Flexibility of Production Manufacturing Processes. In Proceedings of the IEEE 21st International Conference on Intelligent Engineering Systems (INES), Larnaca, Cyprus, 20–23 October 2017. [CrossRef]
22. Koumboulis, F.N.; Fragkoulis, D.G.; Ioannou, K.A. Control of Router Nodes in Production Manufacturing Processes. In Proceedings of the 2018 7th International Conference on Systems and Control (ICSC), Valencia, Spain, 24–26 October 2018; pp. 372–377. [CrossRef]
23. Koumboulis, F.N.; Fragkoulis, D.G.; Diveris, G.K. Function Supervisors for Storage Systems. In Proceedings of the International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, Greece, 7–9 May 2018. [CrossRef]
24. Ruiz-Carcel, C.; Starr, A. Data-Based Detection and Diagnosis of Faults in Linear Actuators. *IEEE Trans. Instrum. Meas.* **2018**, *67*, 2035–2047. [CrossRef]

25. Li, D.; Wang, Y.; Wang, J.; Wang, C.; Duan, Y. Recent advances in sensor fault diagnosis: A review. *Sens. Actuators A Phys.* **2020**, *309*, 111990. [CrossRef]
26. Luo, B.; Wang, H.; Liu, H.; Li, B.; Peng, F. Early Fault Detection of Machine Tools Based on Deep Learning and Dynamic Identification. *IEEE Trans. Ind. Electron.* **2019**, *66*, 509–518. [CrossRef]
27. Wang, H.; Lu, S.; Qian, G.; Ding, J.; Liu, Y.; Wang, Q. A Two-Step Strategy for Online Fault Detection of High-Resistance Connection in BLDC Motor. *IEEE Trans. Power Electron.* **2020**, *35*, 3043–3053. [CrossRef]
28. Najafabadi, T.A.; Salmasi, F.R.; Jabehdar-Maralani, P. Detection and Isolation of Speed-, DC-Link Voltage-, and Current-Sensor Faults Based on an Adaptive Observer in Induction-Motor Drives. *IEEE Trans. Ind. Electron.* **2011**, *58*, 1662–1672. [CrossRef]
29. Ben-Gharbia, K.M.; Maciejewski, A.A.; Roberts, R.G. A kinematic analysis and evaluation of planar robots designed from optimally fault-tolerant jacobians. *IEEE Trans. Robot.* **2014**, *30*, 516–524. [CrossRef]
30. Xiao, B.; Yin, S. An Intelligent Actuator Fault Reconstruction Scheme for Robotic Manipulators. *IEEE Trans. Cybern.* **2018**, *48*, 639–647. [CrossRef]
31. Nguyen, V.C.; Le, P.N.; Kang, H.J. An Active Fault-Tolerant Control for Robotic Manipulators Using Adaptive Non-Singular Fast Terminal Sliding Mode Control and Disturbance Observer. *Actuators* **2021**, *10*, 332. [CrossRef]
32. Phan, V.D.; Vo, C.P.; Dao, H.V.; Ahn, K.K. Robust Fault-Tolerant Control of an Electro-Hydraulic Actuator with a Novel Nonlinear Unknown Input Observer. *IEEE Access* **2021**, *9*, 30750–30760. [CrossRef]
33. Zaytoon, J.; Riera, B. Synthesis and implementation of logic controllers—A review. *Annu. Rev. Control* **2017**, *43*, 152–168. [CrossRef]
34. Guo, L.; Vincentelli, A.S.; Pinto, A. A complexity metric for concurrent finite state machine based embedded software. In Proceedings of the 8th IEEE International Symposium on Industrial Embedded Systems (SIES), Porto, Portugal, 19–21 June 2013. [CrossRef]
35. Koumboulis, F.N.; Fragkoulis, D.G.; Kalkanas, I.; Fragulis, G.F. Supervisor Design for a Pressurized Reactor Unit in the Presence of Sensor and Actuator Faults. *Electronics* **2022**, *11*, 2534. [CrossRef]
36. Koumboulis, F.N.; Fragkoulis, D.G.; Arapakis, S. Supervisor design for an assembly line in the presence of faults. In Proceedings of the 27th IEEE International Conference on Emerging Technology and Factory Automation, Stuttgart, Germany, 6–9 September 2022. [CrossRef]
37. Kučera, E.; Haffner, O.; Drahoš, P.; Cigánek, J. Educational Case Studies for Pilot Engineer 4.0 Programme: Monitoring and Control of Discrete-Event Systems Using OPC UA and Cloud Applications. *Appl. Sci.* **2022**, *12*, 8802. [CrossRef]
38. Ioana, A.; Korodi, A. DDS and OPC UA Protocol Coexistence Solution in Real-Time and Industry 4.0 Context Using Non-Ideal Infrastructure. *Sensors* **2021**, *21*, 7760. [CrossRef]
39. Leitão, H.A.S.; Rosso, R.S.U.; Leal, A.B.; Zoitl, A. Fault Handling in Discrete Event Systems Applied to IEC 61499. In Proceedings of the 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 8–11 September 2020. [CrossRef]
40. Zhong, Z.; Zhang, J.; Qiu, C.; Huang, S. Design of a Framework for Implementation of Industrial Robot Manipulation Using PLC and ROS 2. In Proceedings of the 2022 2nd International Conference on Computer, Control and Robotics (ICCCR), Shanghai, China, 18–20 March 2022; pp. 41–45. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.