# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

186,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities


WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

## Interested in publishing with us?
## Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

25

# A Systematized Approach to Obtain Dependable Controller Specifications for Hybrid Plants

Eurico Seabra and José Machado
*Mechanical Engineering Department, CT2M Research Centre, University of Minho*
*Portugal*

## 1. Introduction

This chapter focuses on the problem that a designer of an automation system controller must solve related with the correct synchronization between different parts of the controller specification when this specification obeys a previously defined structure. If this synchronization is not done according to some rules, and taking some aspects into consideration, some dependability aspects concerning the desired behaviour for the system may not be accomplished. More specifically, this chapter will demonstrate a systematized approach that consists of using the GEMMA (Guide d`Etude des Modes de Marches et d`Arrêts) (Agence Nationale pour le Developpement de la Production Automatisée) [ADEPA], 1992) and the SFC (Sequential Function Chart) (International Electrotechnical Commission [IEC], 2002) formalisms for the structure and specification of all the system behaviour, considering all the stop states and functioning modes of the system. The synchronization of the models, corresponding to the controller functioning modes and the controller stop states, is shown in detail and a systematized approach for this synchronization is presented. For this the advantages and disadvantages of the vertical coordination and horizontal coordination proposed by the GEMMA formalism are discussed and a case study is presented to explain the proposed systematic approach. A complete safe controller specification is developed to control a hybrid plant. Also this chapter presents and discusses a case study that applies a global approach for considering all the automation systems emergency stop requirements. The definition of all the functioning modes and all the stop states of the automation system is also presented according the EN 418 (European Standard [EN], 1992) and EN 60204-1 (EN, 1997) standards. All the aspects related to the emergency stop are focused in a particular way. The proposed approach defines and guarantees the safety aspects of an automation system controller related to the emergency stop. For the controller structure the GEMMA methodology is used; for the controller entire specification the SFC is used and for the controller behaviour simulation the Automation Studio software (FAMIC, 2003) is used.

In order to achieve the goals presented above, the chapter is organized as follows: section 1 presents the challenge addressed to this chapter; in section 2 the main formalisms and methodologies used to define the controller behaviour specification are presented, namely, showing how to deal with complex specifications before the implementation into a physical controller device to help the designer to improve the specifications performance; section 3

discusses different possible approaches for using the coordination of a controller specification when this specification is previously structured by the use of the GEMMA method. This is often applied because the complexity of the specification behaviour demands a separate modular specification, named "task", corresponding to the functioning or failure modes or stop states of the automation system; section 4 presents a case study and shows in detail defining and structuring a controller specification; section 5 presents and illustrates how to coordinate a complex specification applied to a case study with possible extrapolation for similar cases; section 6 is exclusively devoted to the discussion of different possibilities for emergency stop application; further section 7 presents and discusses an example of emergency stop application and, finally, section 8 presents some conclusions.

## 2. Formalisms used to develop the controller behaviour specification

From the desired behaviour specifications, until the implementation of a controller program for an automation system, the controller designer needs to use some different and complementary methods, formalisms and tools that help him in all the necessary steps. Taking into account aspects related to the systems' dependability, the designer must be able to use together these formalisms and tools in order to achieve the desired behaviour for the system. There are many methods, formalisms and tools for helping the designer during all necessary steps. For the structure of the controller it is possible to use the GEMMA method (ADEPA, 1992), Multi-Agent formalism (Sohier, 1996) can be used: for the specification Petri Nets (Murata, 1989), SFC (IEC, 2002), Statecharts (Harel, 1987), UML (Booch et al., 2000) can be used; for the implementation, the PLCs (Programmable logic controllers) (Moon, 1994), Industrial computers (Koornneef and Meulen, 2002), Microprocessors (Brusamolino et al., 1984) and others can be used.

From the analysis of needs, passing by the conception, realization into the implementation and exploitation of an automation system there are several steps that must be realized (Fig. 1). During each step of the controller design a corresponding step of the development of the plant (physical part of the system: motors, cylinders, sensors etc.) exists. For instance, step 3 corresponds to the specification of the controller and step 3' corresponds to the specification of the plant.

The main objective of this chapter is to show how to deal with complex specifications before the implementation into a physical controller device. Usually there are some methods, formalisms and tools that help the designer to improve the specifications performance, but if the coordination of all the parts of the specification is not well done, some aspects related to the dependability of the system may not be accomplished.

This paper applied a case study and then extrapolated to systems of the same kind, in this it is more detailed and more related to steps 3 and 4 presented in Figure 1, than related to the design of a controller.

Currently, some suitable methods and formalisms for the development and creation of the structure and specification of an automated production system controller exist. Among them there are GEMMA (Guide d'Étude des Modes de Marche et d'Arrêt) and SFC (Sequential Function Chart), both developed in France. GEMMA is well adapted to defining the controller structure and SFC is well adapted to complete controller specification.

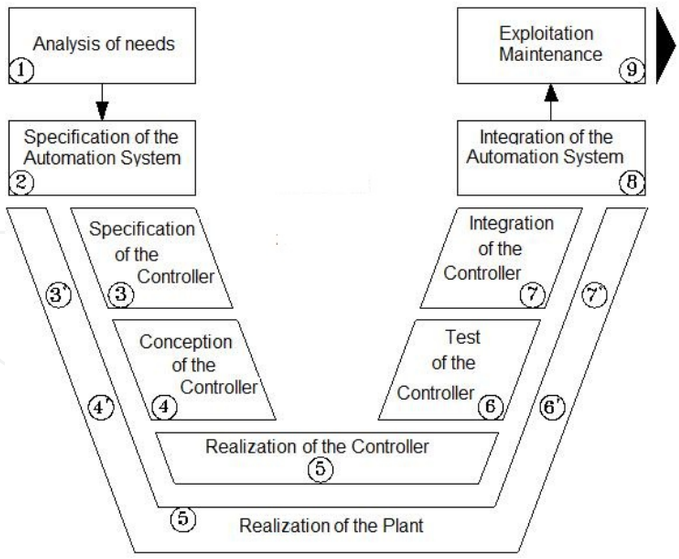



Fig. 1. Steps considered on the design of an automation system

According to SFC rules, the implementation of the automation system requires, in particular, a description relating to cause and effect. To do this, the logical aspect of the desired behaviour of the system will be described. The sequential part of the system, which is accessed via Boolean input and output variables, is the logical aspect of this physical system. The behaviour indicates the way in which the output variables depend on the input. The object of the SFC is to specify the behaviour of the sequential part of the systems. This formalism is characterized, mainly, by its graphic elements, which, associated with an alphanumerical expression of variables, provides a synthetic representation of the behaviour based on a description of the situation of the system.

GEMMA was developed in France by ADEPA (Agence Nationale pour le Developpement de la Production Automatisée) and is a method that on the basis of a very precise vocabulary proposes a simple structured guide for the designer based on a graphical chart that contains all the functioning modes and stop states that a machine or an automated system can assume. It is a tool for helping with system analysis, being used for its supervision, maintenance and evolution definition.

The GEMMA method is based in three basic concepts:

- The operating modes are seen, from the point of view of the command module, as always available. All the systems are composed by a command module and an operative module. In the application of GEMMA, it is assumed that the command module is always on power.
- The production criteria. Two states are considered for the production systems: ON production and OUT of production. Those states are shown on the graphical chart of the method.
- The three groups of functioning modes and stop states of the plant, namely:
  - States “A”: Stop states
  - States “D”: Failure modes
  - States “F”: Running modes

The graphical chart of GEMMA is composed of three parts, each one corresponding to each group of functioning modes and stop states described in Figure 2.

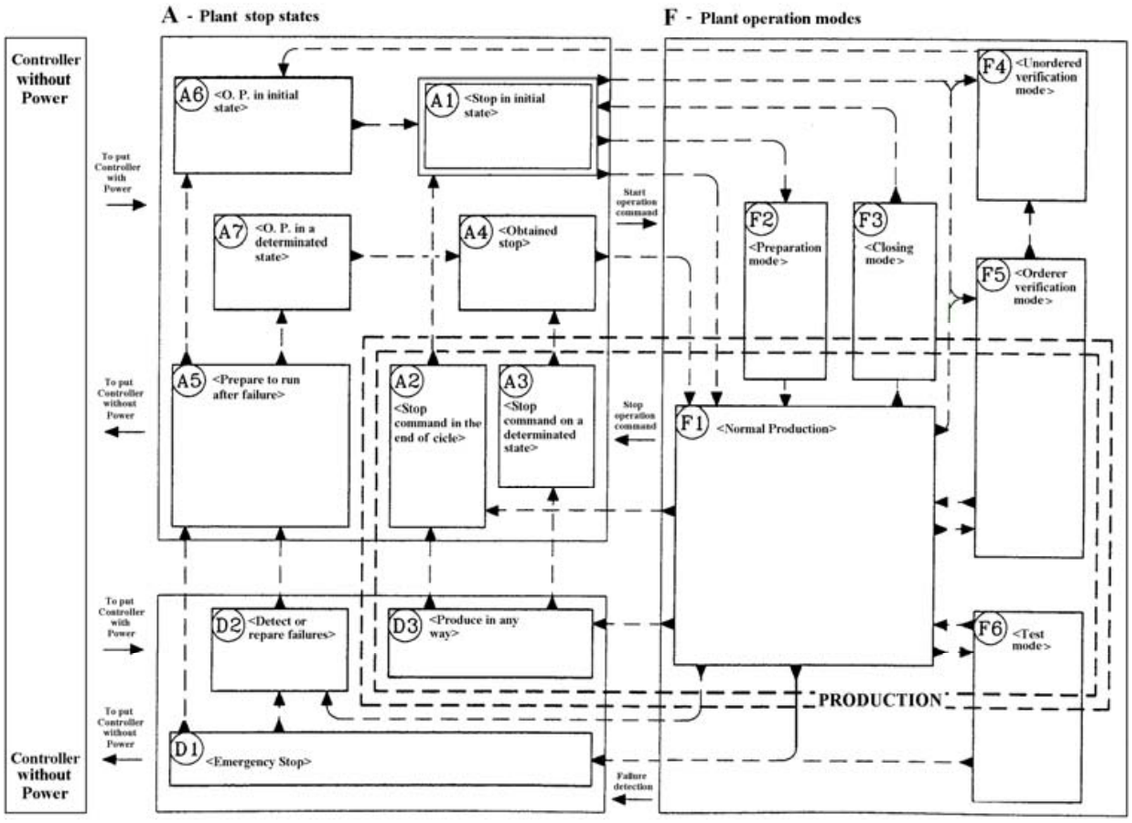



Fig. 2. Functioning modes and stop states considered on the design of an automation system

## 3. Coordination of a complex specification

Very often modes other than F1 (Normal Production Mode) demand a specification behaviour with complex cycles and this complex specification demands also a specific treatment for each of the functioning or failure modes or stop states of the automation system.

So, it seems useful to separate each modular specification corresponding to each of the functioning or failure modes or stop states of the automation system. Each specification module is named "task": a task is associated with the F1 mode, other tasks to the F2 mode and so on for all the functioning and failure modes and stop states of the automation system.

From a practical point of view, and for implementation of SFC, the division of tasks is particularly adapted to these needs and it is possible to make the correspondence between a mode/state, the respective SFC and the respective task, based on the specification SFC for the corresponding mode (Fig. 3).

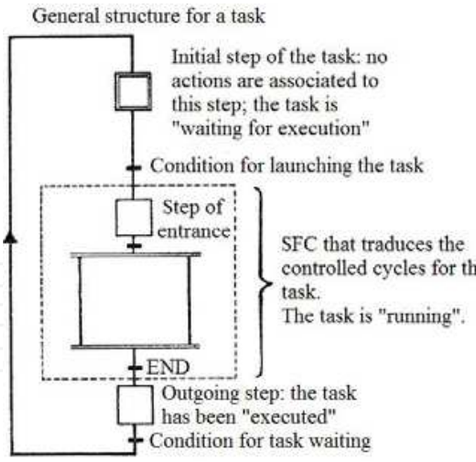



Fig. 3. Structure of a task

### 3.1 Horizontal coordination

This is a very interesting way of coordinating tasks because any task can be dominant over the others and also each task may launch other tasks (Fig. 4).

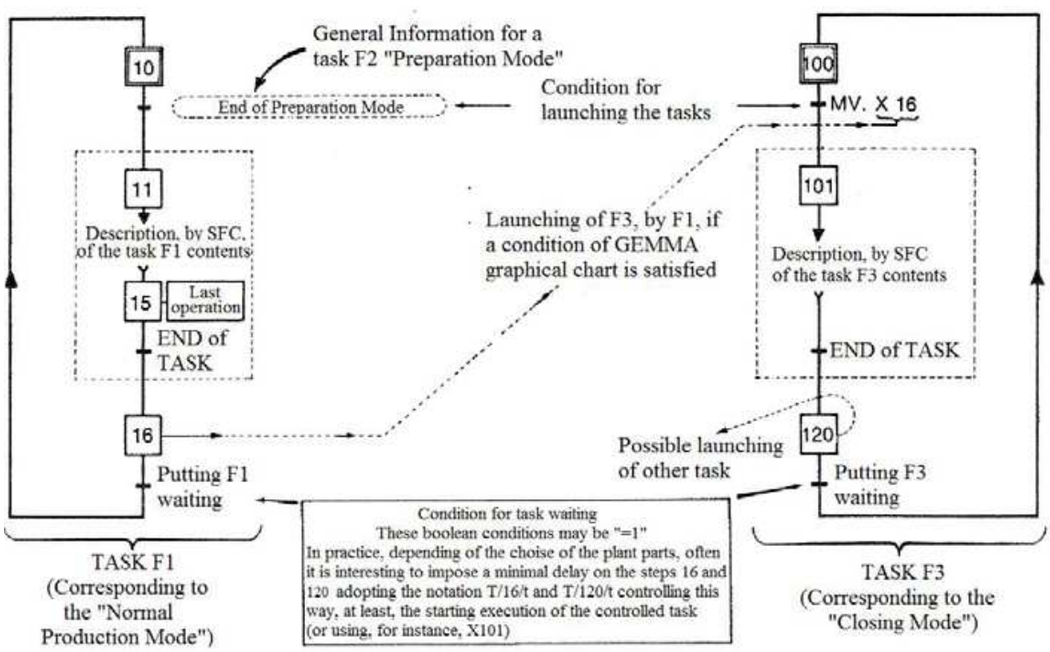



Fig. 4. Horizontal coordination

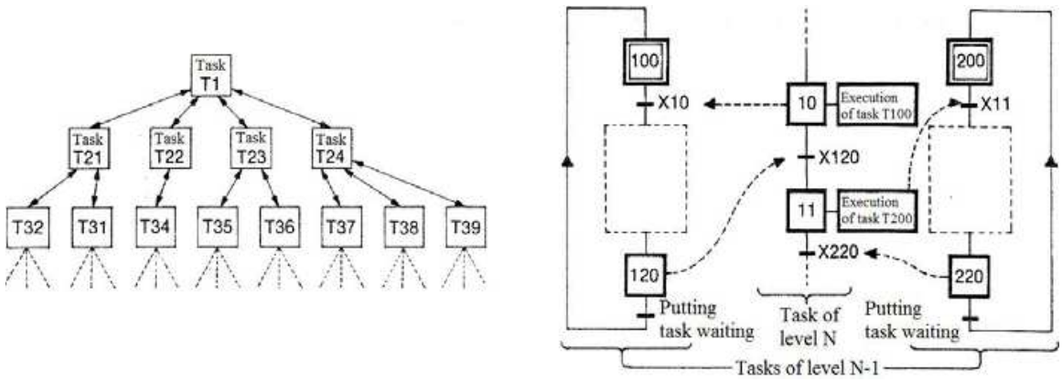
Let's consider a generic task F1 (normal production mode) and a generic task F3 (closing mode). As F3 appears after task F1, F1 must launch F3. When F1 ends (step 16) the Boolean variable X16 makes possible the evolution of the task F3, from the step 100 to the step 101. At the end of task F3 (step 120) the next task is launched by the Boolean variable X120 and so on with similar behaviour, task by task. The variables X*i* are Boolean variables associated to step *i* defined by (IEC, 2002).

### 3.2 Vertical coordination

This kind of coordination is hierarchic and there are several levels of abstraction. Each task of an abstraction level may launch any other task at a lower level, but - on the same abstraction level – one task cannot launch other tasks that belong to the same level (Fig. 5).

With this hierarchical approach the designer may have a global overview of the system and also, if he intends so, a very detailed local view of the system.

The synchronization process is illustrated in a very detailed way in Figure 5 and the SFC of higher level coordinates, at the specific order, indicates the evolution of each task. After the end of each task, the higher level SFC evolutes and, on its next steps, it will launch another task – of the inferior abstraction level - and so on.




a) b)

Fig. 5. Vertical coordination

This approach is easier to systematize and also better adapted to treat more complex systems because of the use of different abstraction levels.

## 4. Case study

The case study corresponds to an automatic machine for filling and capping bottles (Fig. 6). This is divided in three modules, transport and feeding, filling and capping. For increasing productivity, a conveyor is used with several alveoli for the bottles, allowing the operation simultaneously at three working stations (modules of the automation system).

The transport and feeding station is composed of a pneumatic cylinder (A) that is responsible for feeding the bottles to the conveyor and another pneumatic cylinder (B) that executes the step/incremental advance of the conveyor.

The filling module is composed of a volumetric dispenser, a pneumatic cylinder (C) that actuates the dispenser and an on/off valve (D) for opening and closing the liquid supply.

The capping station has a pneumatic cylinder (G) to feed the cover, a pneumatic motor (F) to screw on the cover and a pneumatic cylinder (E) to advance the cover. The cylinder (E) moves forward until the existent cover retracts with this cover during the retraction of (G), and it moves forward again with rotation of the motor F to screw on the cover.

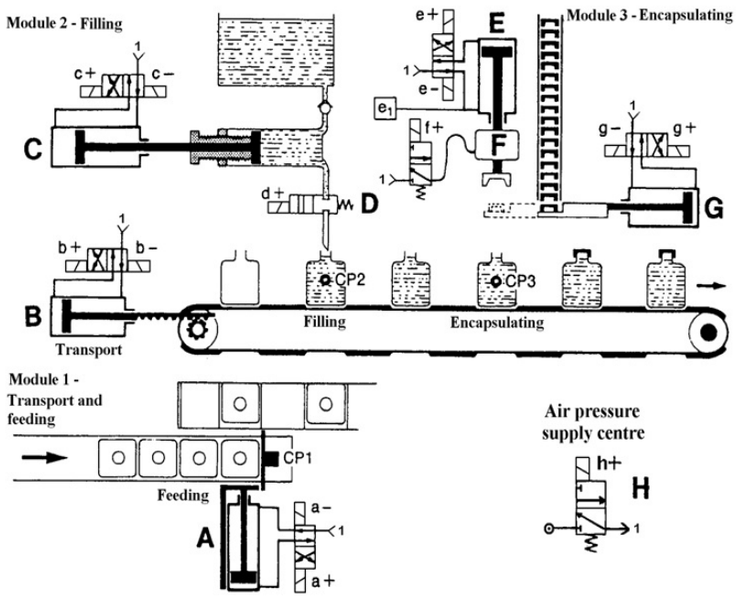



Fig. 6. Case study plant

### 4.1 Base controller behaviour specification

Figure 7 shows the base SFC of the system controller, corresponding only to the "normal production" mode. The basic sensors involved are: two end-course-sensors for each cylinder (example: cylinder A, sensor a0 and a1, respectively, retracted and forward) and a sensor of pressure e1, which detects the point of contact/stop of the cylinder E in any point of its course.

Valve D and motor F do not have position sensors because they are difficult to implement. On the other hand, in order to obtain the total SFC controller, which includes all the operation modes required for the correct operation of the system, the graphic chart of GEMMA was used because it allows definition of the functioning (operation) modes and stop states of the machine.

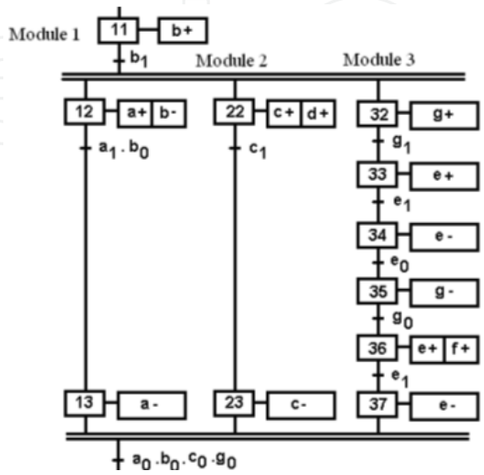



Fig. 7. Base SFC controller specification

### 4.2 Global controller structure

Figure 8 shows the GEMMA graphic chart developed for the presented case study. The considered tasks are described as follows:

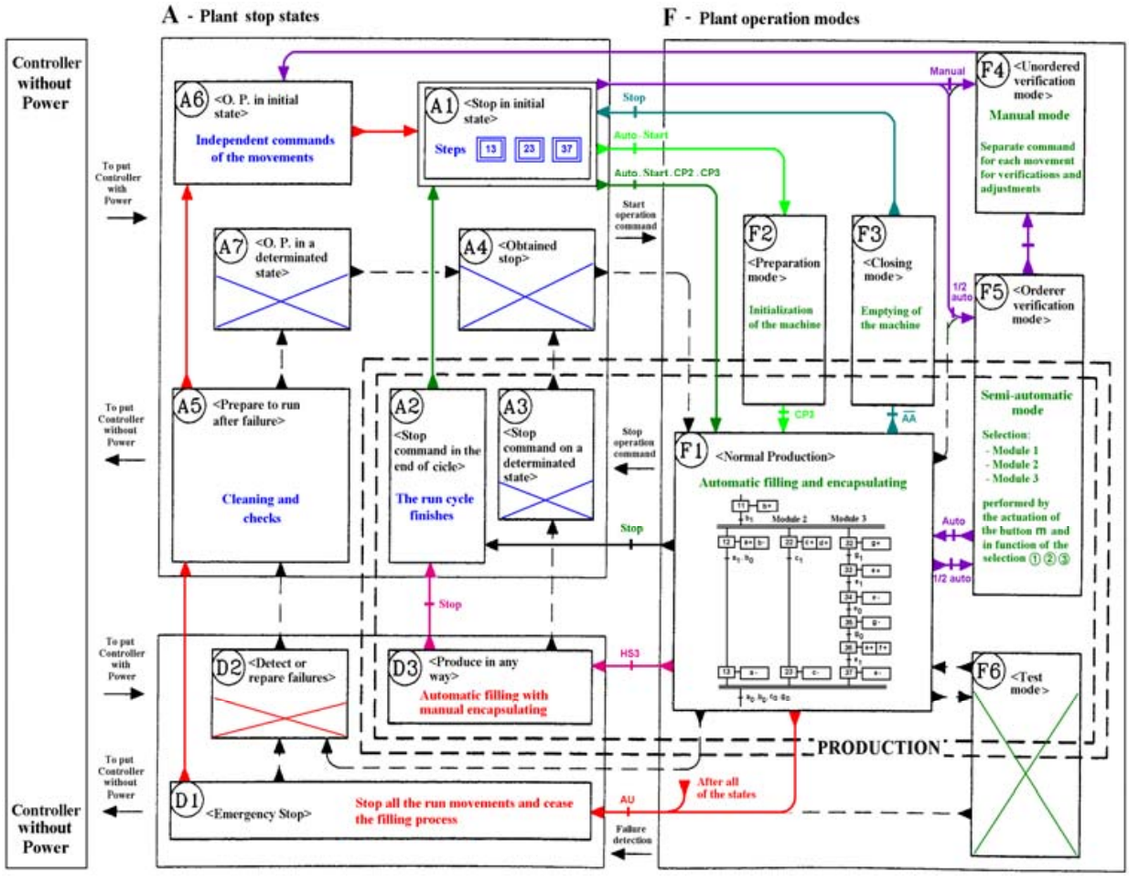



Fig. 8. GEMMA of the plant controller

A1 – The task A1 "stop in the initial state" represents the task of the machine represented in Figure 8.

F1 – Start of task A1, when the start command of the machine occurs, the change for the task F1 "normal production" happens (filling and automatic capping) with the consequent execution of base SFC presented in Figure 7.

A2 – When happens the stop command of the machine happens, the run cycle finishes in agreement with the condition described at task A2 "stop command at the end of cycle".

F2 – When the machine is "empty" (without bottles) it is necessary to feed bottles progressively, the machine being ready to begin the normal production (task F1) when it has bottles in the conveyor positions of the production modules 2 and 3, respectively. This operation is defined by task F2 "preparation mode".

F3 – The "closing mode" of task F3 allows the reverse operation, that is, the progressive stop of the machine with the exit of all of the bottles (emptying of the machine).

D3 – When the capping module is out of service it can be decided to produce in another way, that is, to perform the bottle filling in an automatic way and posterior manual capping, this is the main purpose of task D3 "production in another way".

D1 – In the case of a situation emergency, task D1 "emergency stop" is executed. This stops all the run actions and closes the filling valve to stop the liquid supply.

A5 – After the emergency stop (task D1), cleaning and verification are necessary: this is the purpose of task A5 "prepare to run after failure".

A6 –After the procedures of cleaning and verification finish it becomes necessary to perform the return to the initial task of the machine, as described at the task A6 "O.P. (operative plant) in the initial state".

F4 – For example, for volume regulation of the bottle liquid dispenser and adjustment of the bottle feeder, a separate command for each movement is required, according to task F4 "unordered verification mode".

F5 – For detailed operation checks, a semiautomatic command (only one cycle) it is necessary to check the functioning of each module: task F5 "ordered verification mode".

To make this possible GEMMA evolution becomes necessary, creating transition conditions for the run and stop operation modes, as described previously.

These transition conditions will be accomplished using GEMMA, as presented, to proceed:

- To allow the progressive feeding demanded in the preparation way (F2) and the progressive discharge required in the closing way (F3) it will be necessary to consider sensors that detect the bottles' presence under each one of the modules 1, 2, 3, respectively, CP1, CP2, CP3 (see Fig. 6);
- Also, it will be necessary a command panel that supplies the transition conditions given by an operator (Fig. 9).

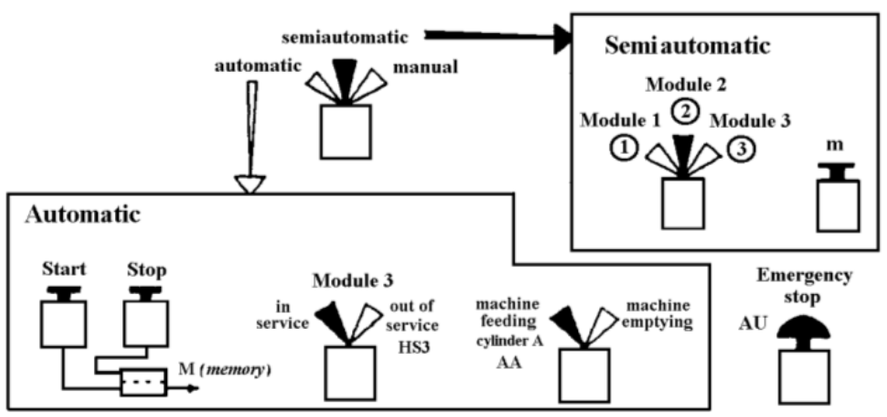



Fig. 9. Command panel of the system controller

In the command panel, there is a main switch that allows selecting the "automatic", "semiautomatic" and "manual" operation modes.

"Automatic" option corresponds to:

- Two buttons, "start" and "stop", whose actions are memorized in memory M;
- A switch HS3 to put module 3 "in service" or "out of service";
- A switch AA to control the bottles' feeding permission (cylinder A), to allow the emptying of the machine.

These switches/buttons and sensors CP1, CP2 and CP3 are the transition conditions of the tasks A1, F1, F2, F3, A2 and D3, as shown in Figure 8.

The "semiautomatic" option corresponds to task F5 "ordered verification mode" which allows the actuation of button (m) to check one cycle operation of each module selected by the "semiautomatic" switch ①,②, or ③.

The "manual" option corresponds to tasks F4, A5 and A6, which require a separate command from each movement using a direct command on the directional valves.

Finally, the AU button (emergency stop) allows passing to task D1 which starts from all of the tasks.

## 5. Coordination of the case study's complex specification

The implementation of total controller specification, based on GEMMA presented in Figure 8, can be realized using the following two alternative methods, when one SFC for each task is developed (Multiple SFC):

- Horizontal coordination;
- Vertical coordination.

As shown in section 3, there are several aspects/benefits for each described implementation (vertical coordination and horizontal coordination). However, it seems to be more systematic for vertical coordination because two levels of abstraction can be defined and when the system is really complex, this aspect seems to be very helpful.

Figure 10 shows the schema of the adopted approach for the case study (vertical coordination).

According Figure 10, GEMMA implementation is performed based on the following main stages:

1. Elaboration of a high level SFC that directly translates the base GEMMA of the system behaviour;
2. Elaboration of multiple low level SFCs corresponding to each functioning mode and/or stop state;
3. Synchronization of the SFCs using the vertical coordination methodology.

### 5.1 High level SFC

This is the first stage of the vertical coordination implementation of total controller specification. Figure 11 shows the high level SFC that directly corresponds to the base GEMMA of the case study plant controller presented previously in the Figure 8.

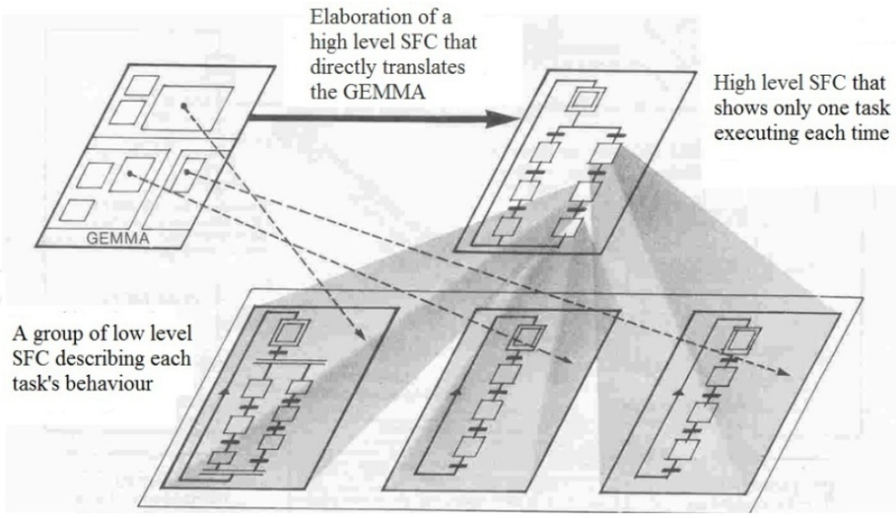



Fig. 10. GEMMA implementation with vertical coordination of multiple SFC

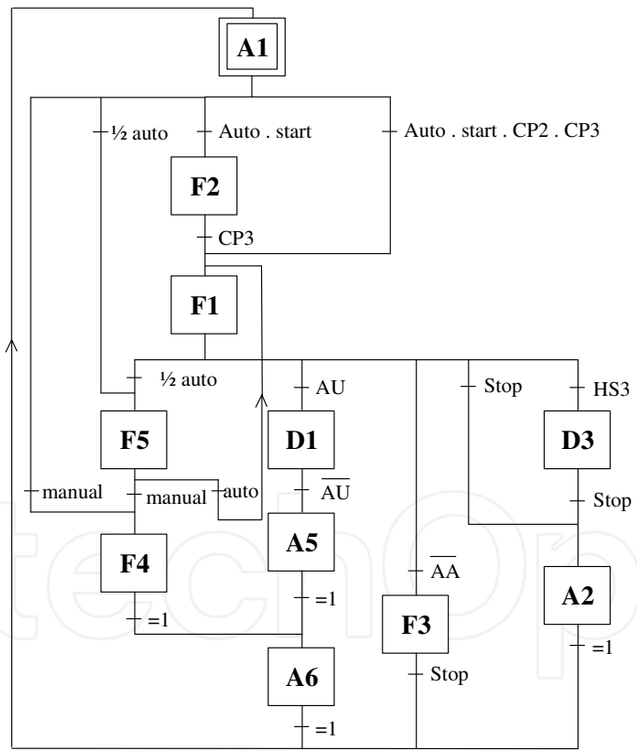
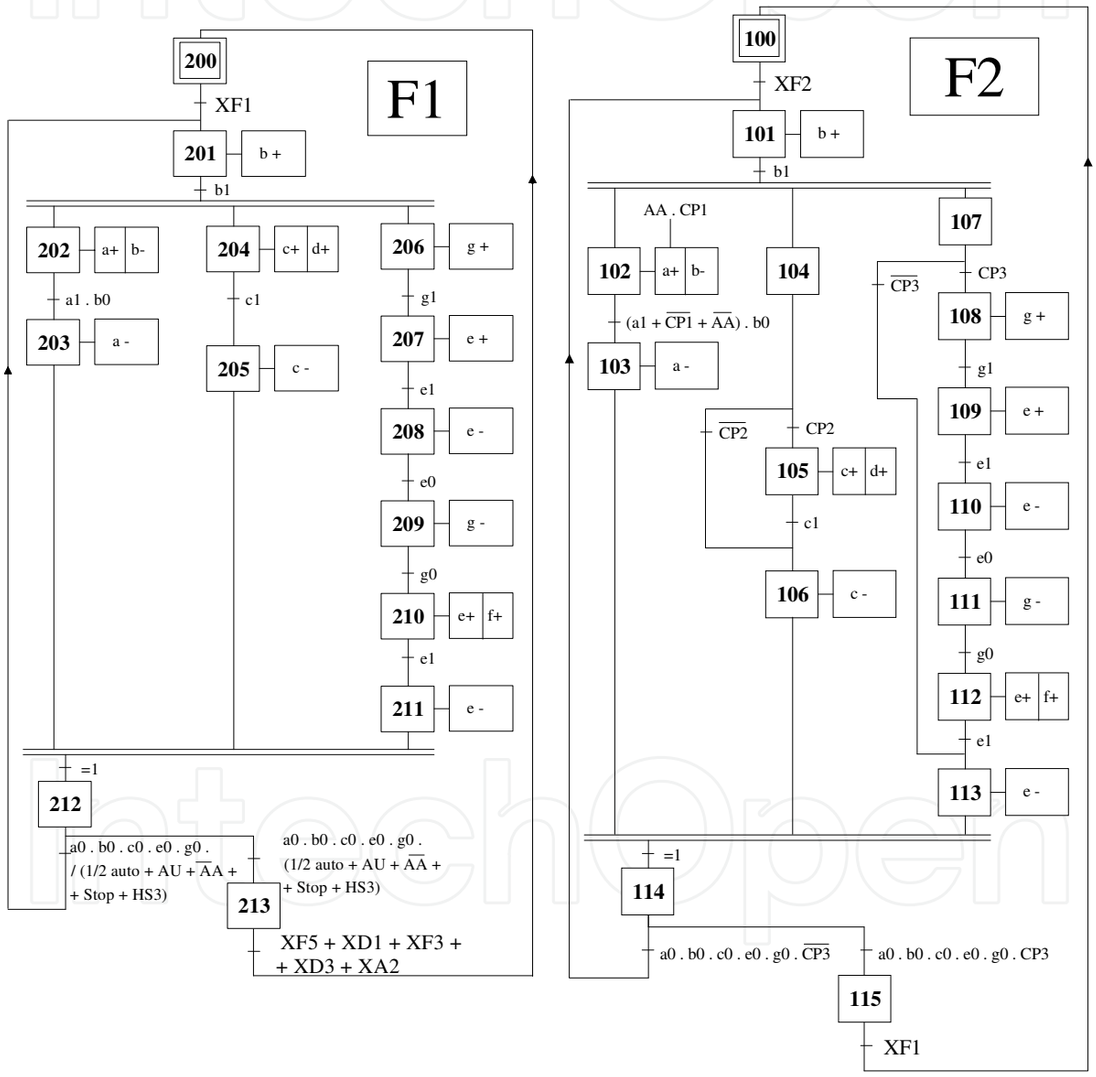



Fig. 11. High level SFC

### 5.2 Low level SFCs

The development of multiple low level SFCs specifications, corresponding to each one of the functioning modes and/or stop states considered for the case study plant controller, is the second stage of the vertical coordination implementation of total controller specification.

In this chapter, the SFCs' specifications corresponding to each one of the functioning modes and/or stop states will be shown. As mentioned before, when using the GEMMA approach, each SFC corresponding to each functioning mode and/or stop state is treated as a task. In this way, Figure 12 shows the SFC specification for the tasks F1 "normal production" and F2 "preparation mode". The SFC of the task F3 "closing mode" is not shown because it is similar to that presented for task F2. Additionally, Figure 13 shows the SFC specification for tasks F5 "ordered verification mode" and D3 "production in another way".

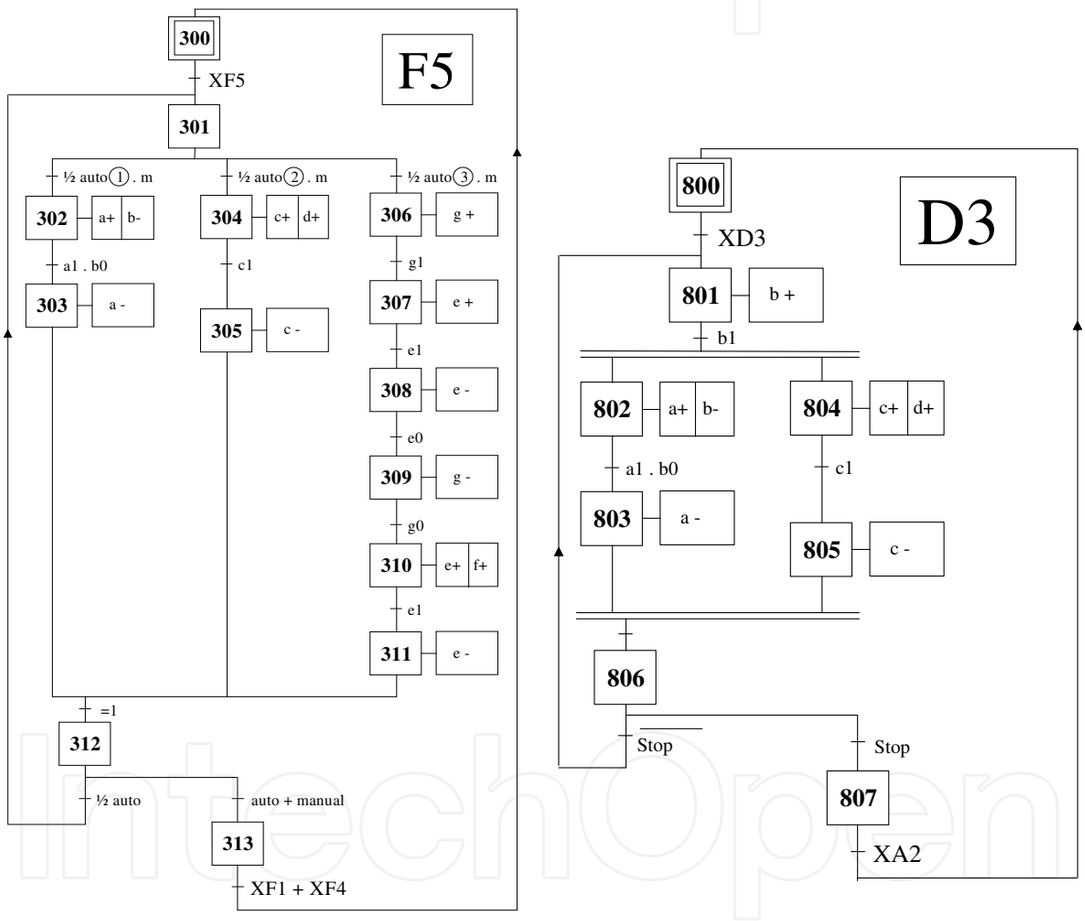



a) b)

Fig. 12. a) Low level SFC for the normal production task, and b) low level SFC for the preparation task

It is of importance to note that the "emergency stop" related to GEMMA task D1 is not treated in this section due to its complexity. The "emergency stop" controller behaviour specification will be presented in detail in sections 6 and 7 of this chapter. In particular, section 7 presents and discusses the implementation of GEMMA task D1 of the same case study (Fig. 8), with the aim of applying a global approach considering all automation system emergency stop requirements.

The definition of all functioning modes and all stop states of the automation system were performed according European standards EN 418 (EN, 1992) and EN 60204-1 (EN, 1997).




a) b)

Fig. 13. a) Low level SFC for the ordered verification task, and b) low level SFC for the production in another way task.

### 5.3 SFCs synchronization

The last stage of the vertical coordination implementation of total controller specification is related to the synchronization of the low level SFC specifications.

To achieve this as described in section 2, the high level SFC presented in Figure 14 was completed with the SFC step activity/action (Xi - i step number) that correspond to the low level SFC execution stop. Figure 14 shows the complete high level SFC obtained for vertical coordination implementation (the SFC step activities added are represented in red).

All the controller specifications, presented in the previous figure, were simulated on Automation Studio software. The obtained results led to the conclusion that all the requirements defined on the Emergency Stop Standards were met.

Further, the specification was translated to Ladder Diagrams according to the SFC algebraic formalization and implemented on a Programmable Logic Controller (PLC) adopted as the controller physical device. This part of the developed work is not detailed in this chapter.

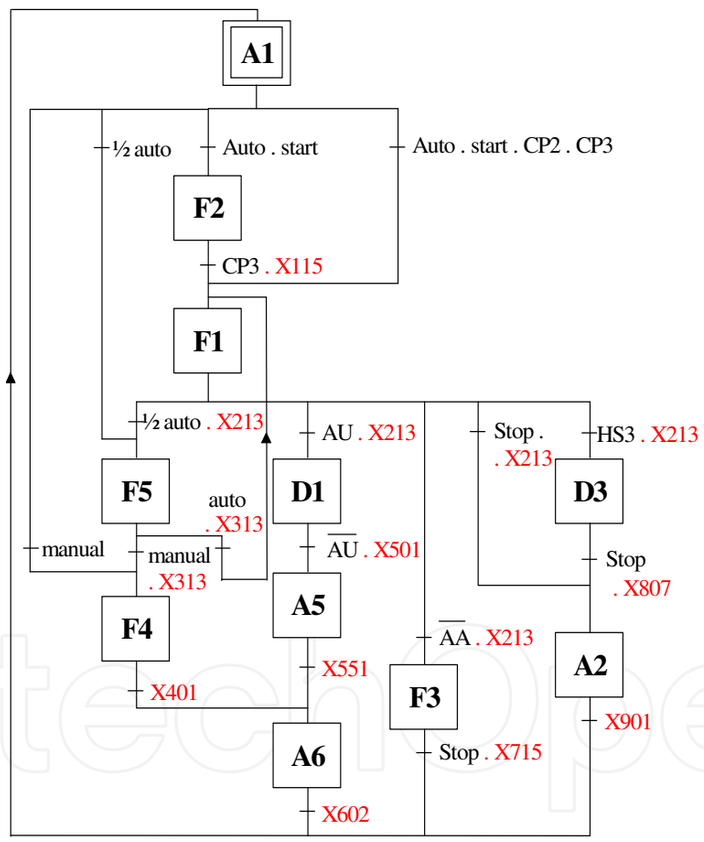



Fig. 14. High level SFC completed with low lever SFC step activities (in red).

All the SFC controller specifications, presented in the previous Figure, were simulated on Automation Studio software (FAMIC, 2003). The obtained results led to the conclusion that all of the automation system requirements were met.

Further, the specification was translated to Ladder Diagrams according to the SFC algebraic formalization (IEC, 2002) and implemented on a Programmable Logic Controller (PLC)

adopted as the controller physical device. This part of the developed work is not detailed in this publication.

## 6. Emergency stop controller behaviour specification

The Emergency Stop is one of the most important aspects related to the safety of people, goods and equipments that interact with automated systems.

In order to obtain safe controllers, it must obey some rules (EN, 1992), (EN, 1997):

- A fault in the software of the control system must not lead to hazardous situations;
- Reasonably foreseeable human error during operation must not lead to hazardous situations;
- The machinery must not start unexpectedly;
- The parameters of the machinery must not change in an uncontrolled way, where such change may lead to hazardous situations;
- The machinery must not be prevented from stopping if the stop command has already been given;
- No moving part of the machinery or piece held by the machinery must fall or be ejected;
- Automatic or manual stopping of the moving parts, whatever they may be, must be unimpeded;
- The safety related parts of the control system must apply in a coherent way to the whole of an assembly of machinery and/or partly completed machinery;

The above mentioned rules can be seen as very important and they must be accomplished by the system behaviour and must be guaranteed by the controller program. However, the ways that designers use to achieve these goals can change. For instance, it can depend on the complexity of the system: if the system is more complex, then the implementation of the emergency stop requirements can be harder. Some indications can be done to the designers, but the final decision depends always of his/her scientific and technical background. This means that different solutions – for application of the emergency stop requirements - can lead to the same practical results. Also, some indications can be done - according to the different ways of guaranteeing the emergency stop requirements – such as if it is necessary, or not, a specific SFC for modelling the behaviour of the system after the emergency stop actuation. Sometimes a specific SFC for modelling the behaviour of the system is necessary after the emergency stop actuation and sometimes it is not.

From this last point of view, the types of emergency stops are divided in two main groups:

- Without emergency sequence - the actuation of the emergency button stops the system/automatism through the inhibition of the outputs and/or for stop the evolution of SFC.
- With emergency sequence - the actuation of the emergency button starts a particular predefined procedure.

As guarantee that the developed controller will always react according the expected behaviour, it is only necessary to model the controller and the plant discretely. Indeed, our system has a hybrid plant, but the behaviour properties that we intend to guarantee for our system are only related to discrete behaviour.

### 6.1 Without emergency sequence

The emergency without emergency sequence can be performed in three alternative modes:

- Outputs inhibition;
- Evolution stop;
- Outputs inhibition and evolution stop.

In the case of outputs inhibition the actuation of emergency button does not stop by itself the evolution of the SFC controller, but it inhibits the outputs associated with their steps, as shown in Figure 15. The ON outputs (state 1) are turned OFF (state 0), as well as the evolution of SFC usually being stopped by the non-fulfilment of the logical conditions associated with SFC transitions.

This can be obtained through the insertion of inhibition functions in the interface with the machine plant. In this case, after the occurrence of an emergency stop, the actuator's command should be particularly well studied in agreement with the type of expected response.

For instance, for the cylinders directional valves:

- One stable state valve (single control with spring return), if a cylinder return for a given position is demanded.
- Two stable state valve (double control), if a stop at the end of the cylinder movement is demanded.
- Valve with three positions (double control and spring return), if a cylinder stop in the actual position is demanded.

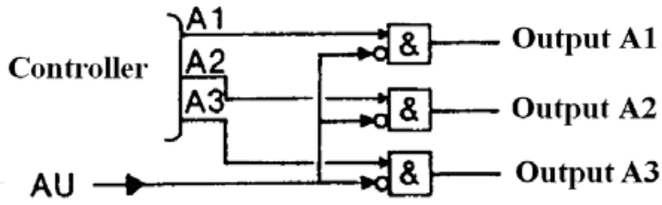


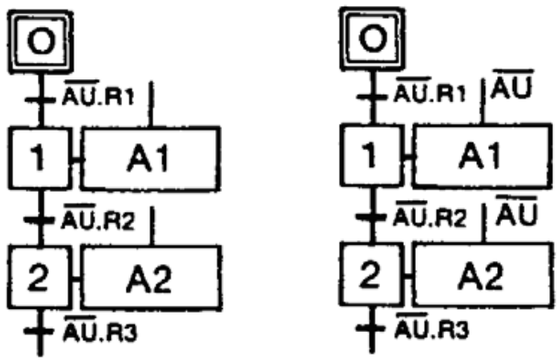

Fig. 15. Functional diagram of output inhibition

In the other hand, in the case of evolution stop the condition AU is present in all logical conditions associated with SFC transitions(Fig.16-a). With the actuation of emergency button AU, no logical conditions associated with SFC transitions can be validated and in this way, the controller SFC cannot step forward. With the AU shutdown, a new cycle evolution is allowed.

It is of importance to note that in this situation the outputs associated to the active steps stay validated. This way, the started actions can be maintained, if dangerous situations are not to occur.

Finally, also it is possible to use the described types of emergency stop simultaneously, without emergency sequence, outputs inhibition and evolution stop (Fig. 16-b). This

situation is used more in practice, if a specific emergency sequence is not necessary. Seen that has the advantage of allowing, after the emergency button shutdown, the pursuit of the evolution of the system starting from the same position at which it was stopped.




a) b)

Fig. 16. a) Evolution stop, and b) evolution stop and outputs inhibition

### 6.2 With emergency sequence

This type of emergency implies the introduction of an emergency sequence. Through the activation of the emergency button AU, an emergency sequence can be added to the normal run SFC (Fig. 17).

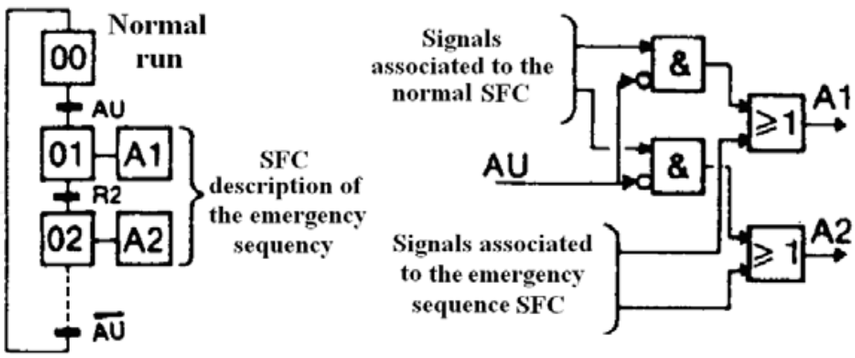



Fig. 17. Introduction of an emergency sequence

## 7. Emergency stop adopted solution: case study

The implementation of total controller specification, based on GEMMA presented in Figure 8, can be realized using the following two main alternative methods:

- Multiple SFC – developing one SFC for each task (implementation of horizontal or vertical coordination);

- Single SFC – developing one SFC for all tasks.

Although this last alternative is possible from a theoretical point of view, for most if not all automation systems practice shows that if the application of emergency stop requirements is done on a complex system, the first solution (multiple SFC) is better.

However, the specification of a specific behaviour for the emergency stop requirements (with emergency sequence) and its linking with other specified behaviours for the system (it doesn't matter if by single or multiple SFCs) is similar. For this reason, this section considers one single SFC for specification of all the desired behaviours for the system. Although the Single SFC method was used for the implementation of the "emergency stop" to allow a better global visualization and understanding of the implementation of the total controller specification that includes the "emergency stop" (GEMMA task D1), it must be highlighted that step 100 of the SFC presented in Figure 5 corresponds to an emergency stop sequence.

The emergency stop adopted for the case study presented was obtained according the EN 418 and EN 60204-1 standards.

According to the behaviour of the case study, the emergency stop with emergency sequence was selected. The considered requirements that need to be accomplished by the emergency sequence are:

- Stop all of the movements;
- Stop the filling operation.

To obtain these procedures the selection of the type of the appropriate directional valves to accomplish, simultaneously, the requirements of the emergency stop and of the plant behaviour was crucial.

The directional valve specifications used were the type of control (single solenoid control with spring return or double solenoid control) and number of ways/ports.

The first security requirement relates to the stop of the movements, obtained by stopping the air compressed supply to the directional valves of the cylinders A, B, C, E, G and of motor F. For that, as shown in Figure 6, the air supply will be centralized and controlled through a directional valve 3/2 way normally closed with spring return (H).

The second security requirement relates to the stopping of the filling operation; this was performed through the turn OFF of the filling directional valve 2/2 way normally closed with spring return (D).

Figure 18 shows the total controller SFC specification based on GEMMA implementation with the single SFC method.

All the SFC controller specifications, presented in Figure 18, were simulated on Automation Studio software. The obtained results led to the conclusion that all the requirements defined in the Emergency Stop Standards were met.

Further, the specification was translated to Ladder Diagrams according to the SFC algebraic formalization and implemented on a Programmable Logic Controller (PLC) adopted as the controller physical device. This part of the developed work is not detailed on this publication.

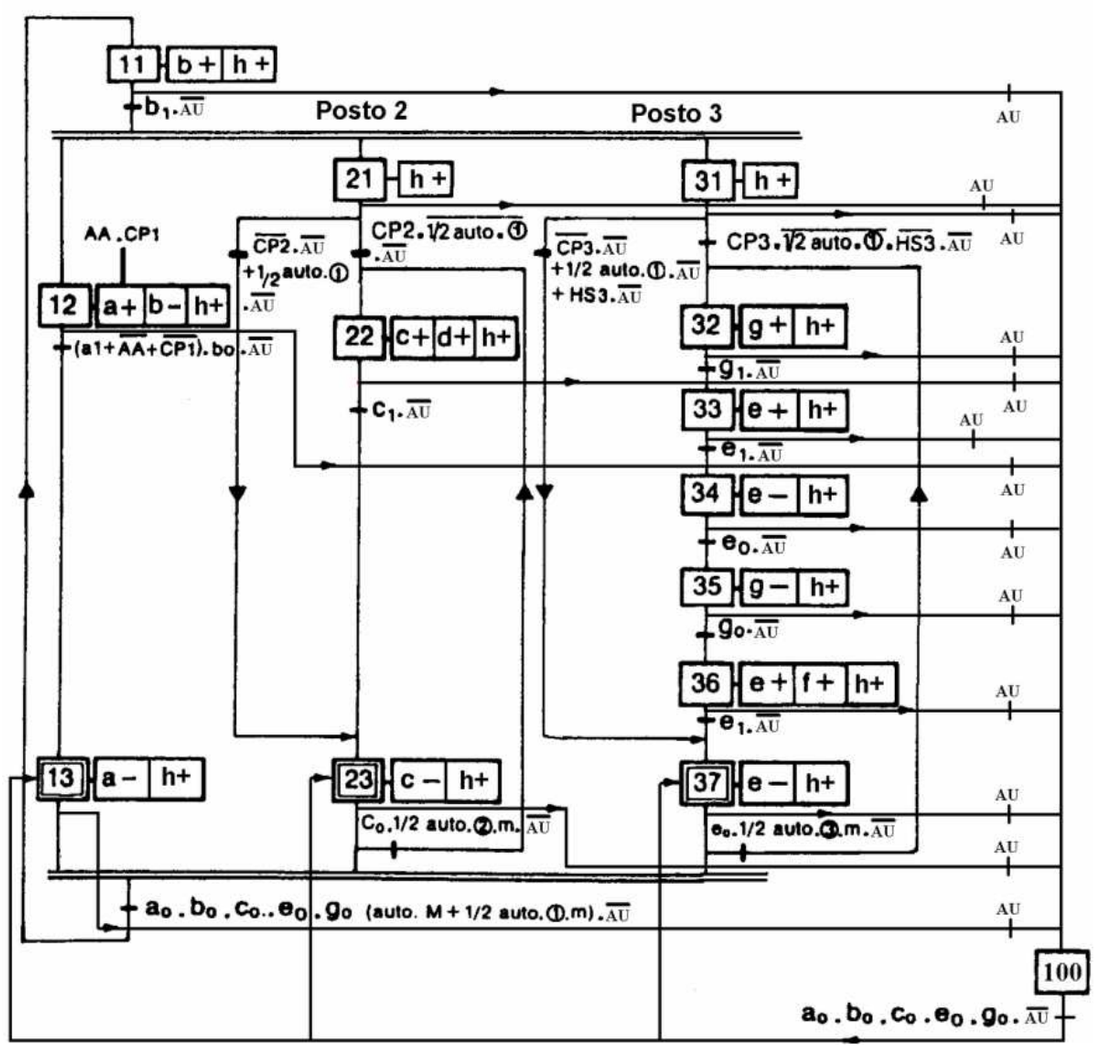



Fig. 18. Total SFC controller specification with emergence sequence

## 8. Conclusions

A systematic way was presented using the adopted techniques for the implementation of complex specifications of automation systems.

First the use of GEMMA and SFC for the structure and specification of all the system's behaviour was explained, considering its stop states and functioning modes.

Further, the vertical coordination implementation of a complex total controller specification, based on the GEMMA graphical chart, was also presented and discussed.

Also, the adopted techniques for the emergency stop behaviour specification of automation systems were presented in a systematic way.

The ways to translate the GEMMA graphical chart to low level specification were also presented and discussed.

The standards (EN418, EN60204-1) related to the stop emergency specifications were considered and all the requirements were accomplished.

The obtained results, by simulation with Automation Studio software, showed that the adopted approach is adequate.

## 9. References

ADEPA (1992). GEMMA - Guide d`Étude des Modes de Marches et d`Arrêts, Ed.2, In: *Agence Nationale pour le Developpement de la Production Automatisée*, France

Booch, G.; Jacobson, I. & Rumbaugh, J. (2000). OMG Unified Modeling Language Specification., In: *Object Management Group edition*, Object Management Group

Brusamolino, M.; Reina, L. & Spalla, M.F. (1984). An example of microprocessor's application in minicomputer systems: a copy volume design and implementation, In: *Microprocessing and Microprogramming*. Vol.13, Issue 5, pp. 331- 339

EN 418 (1992). Safety of machinery. Emergency stop equipment, functional aspects. Principles for design, In: *European Standard*

EN 60204-1 (1997). Safety of Machinery - Electrical Equipment of Machines - Part 1: General Requirements-IEC 60204-1, In: *European Standard*

FAMIC (2003). Automation Studio – User´s Guide, *Famic Technologies Inc*, Canada.

Harel, D. (1987). Statecharts: a visual formalism for complex systems, In: *Science of Computer Programming*, Vol.8, pp 231-274, North Holland, Netherlands

IEC (2002). IEC 60848 - Specification language GRAFCET for sequential function chart, Ed.2, In: *International Electrotechnical Commission*

Koornneef, F. & Meulen, M.V.D. (2002). Safety, reliability and security of industrial computer systems, In: *Safety Science*, Vol.40, Issue 9, pp. 715-717

Moon I. (1994). Modeling Programmable Logic Controllers for Logic Verification, In: *IEEE Control Systems Magazine*, pp. 53-59

Murata, T. (1989). Petri Nets: Properties, Analysis and Applications, *Proceedings of the IEEE*, Vol. 77, No. 4, pp. 541-580, 1989

Sohier, C. (1996). Pilotages des Cellules Adaptatives de Production: Apport des Systemes Multi-Agents, *PhD Thesis*, École Normale Supérieure de Cachan, Paris, France

© 2012 The Author(s). Licensee IntechOpen. This is an open access article distributed under the terms of the Creative Commons Attribution 3.0 License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

IntechOpen

IntechOpen