ABCM Symposium Series in Mechatronics - Vol. 4 - pp.408-417

A SYSTEMATIZED APPROACH TO OBTAIN DEPENDABLE CONTROLLERS SPECIFICATIONS

José Machado, jmachado@dem.uminho.pt
Eurico Seabra, eseabra@dem.uminho.pt
University of Minho, Mechanical Engineering Department, Campus of Azurém, 4800-058 Guimarães, Portugal

Abstract. *This paper is focused on the problem that a designer, of an automation system controller, must solve that is related with the correct synchronization between different parts of the controller specification when this specification obeys at a previous defined structure. If this synchronization is not done according some rules, and taking some aspects in consideration, some dependability aspects, concerning the desired behavior for the system, may not be accomplished. More specifically, it is shown, in the paper, a systematized approach that consists in using the GEMMA and the SFC formalisms for the structure and specification of all the system behavior, considering all the stop states and functioning modes of the system. The synchronization of the models, corresponding of the controller functioning modes and of the controller stop states, is shown in detail and it is presented a systematized approach for this synchronization. For this, there are discussed, on the paper, the advantages and disadvantages of the Vertical coordination and Horizontal coordination proposed by the GEMMA formalism. A case study is presented to explain the proposed systematic approach. A complete safe controller specification is developed to control a hybrid plant.*

Keywords*: Dependable Controllers Design, GEMMA, SFC*

1. INTRODUCTION

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

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 (Figure 1). During each step of the controller development it exists a corresponding step corresponding to the development of the plant. For instance, the step 3 corresponds to the specification of the controller and the step 3' corresponds to the specification of the plant.

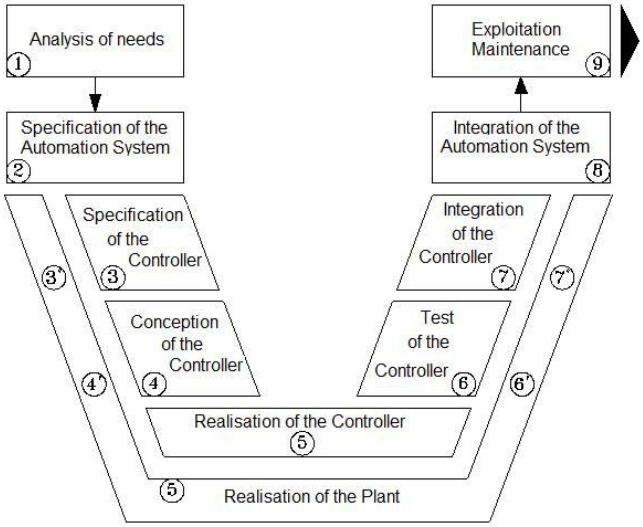

Figure 1. Steps considered on the design of an automation system.

The main idea of this paper is to show how to deal with complex specifications before the implementation into a physical controller device. Usually, there are some formalisms and tools that help the designer to improve the

ABCM Symposium Series in Mechatronics - Vol. 4 - pp.408-417

specifications performance but if the coordination of all the parts of the specification is not well done, some aspects related with the dependability of the system may not be accomplished.

The study here presented, applied to a case study, and then extrapolated to systems of the same kind, is more detailed and more related with the steps 3 and 4 presented in Figure 1, related with the design of a controller.

Currently, there exist some suitable formalisms for the development and creation of the structure and specification of an automated production system controller. Between these formalisms, are distinguished the GEMMA (Guide d'Étude des Modes de Marche et d'Arrêt) (ADEPA, 1992) and SFC (Sequential Function Chart) (IEC, 2002), both developed in France. The GEMMA is well adapted to define the controller structure and SFC is well adapted to the complete controller specification.

According to SFC rules, the implementation of the automation system requires, in particular, a description relating cause and effect. To do this, the logical aspect of the desired behavior 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 behavior indicates the way in which the output variables depend on the input. The object of the SFC is to specify the behavior of the sequential part of the systems. The specification language SFC enables a Grafcet to be created showing the expected behavior of a given sequential system. This tool is characterized mainly by its graphic elements, which, associated with an alphanumerical expression of variables, provides a synthetic representation of the behavior, based on an indirect description of the situation of the system.

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

The GEMMA method is based in three basic concepts:

- The Ways of Run are seen by the command module in the Way of Run. 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. That states are shown on the graphical chart of the method.
- The three groups of run and stop ways or states of the Plant.
  - States "A": Stop states
  - States "D": Failure ways
  - States "F": Running ways

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

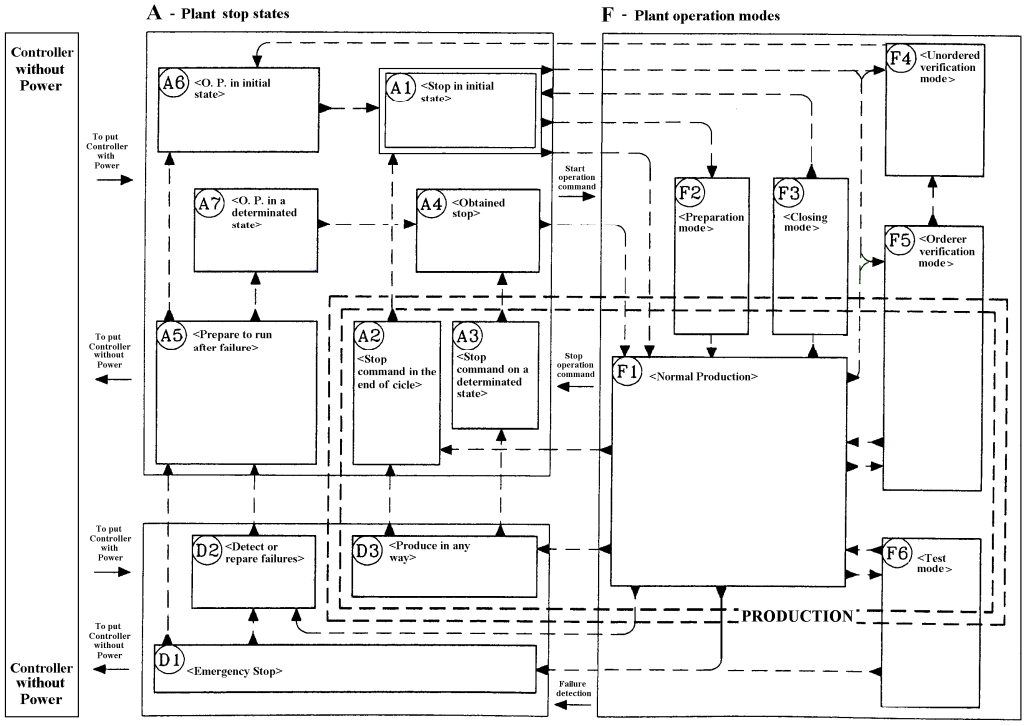

Figure 2. Graphical chart of GEMMA.

ABCM Symposium Series in Mechatronics - Vol. 4 - pp.408-417

In order to achieve the goals presented above, the paper is organized as follows: section 1 presents the challenge addressed to this work; in section 2 there are presented and discussed different approaches possible to use for the coordination of a controller specification when this specification is, previously, structured by the use of GEMMA method; further, section 3 presents a case study and shows, in detail, how defining and structuring a controller specification; followed by section 4 that presents and illustrates how to coordinate a complex specification, applied to the case, study with possible extrapolation for similar cases; and, finally, section 5 presents some conclusions and future works.

2. COORDINATION OF A COMPLEX SPECIFICATION

It happens, very often, that other modes, than F1 (Normal Production Mode), demand a specification behavior 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, each specification module, to each of the functioning or failure modes or stop states of the automation system. Each specification module is named as “task”: it is associated a task to the F1 mode, other task 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 facility of implementation the SFC, the division on 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), Figure 3.

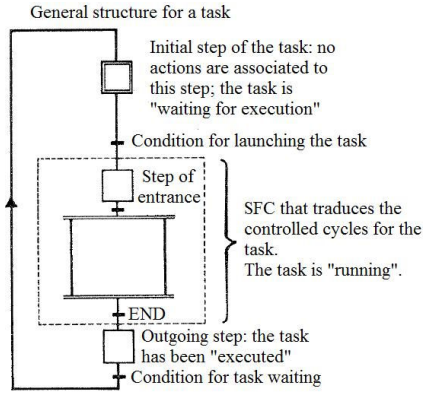

Figure 3. Structure for a task.

2.1. Horizontal Coordination

This is a very interesting way of coordination of tasks because any task is dominant of the others and, also, each task may launch other task (Figure 4).

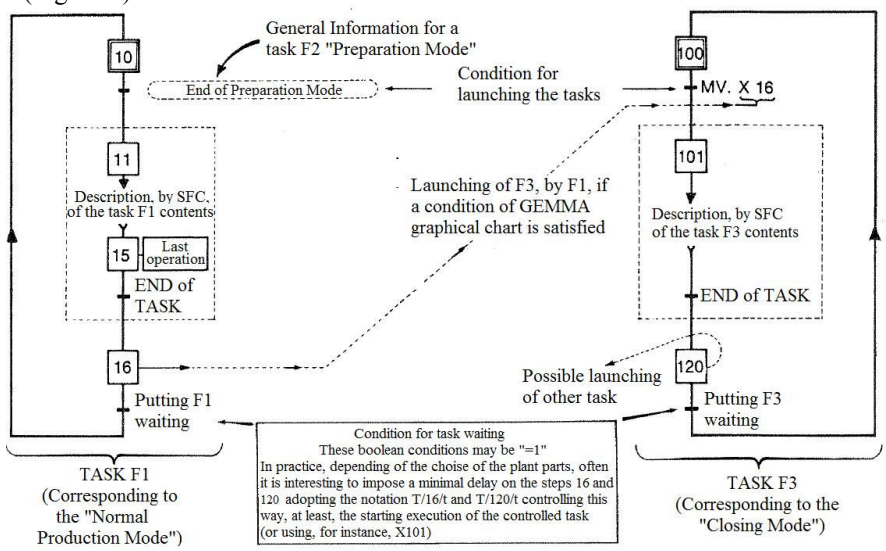

Figure 4. Horizontal coordination

ABCM Symposium Series in Mechatronics - Vol. 4 - pp.408-417

Let's consider a generic task F1 (normal production mode) and a generic task F3 (closing mode), Figure 4. In this case, the task F3 appears after the task F1, so 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. In the end of the task F3 (step 120) the next task is launched by the Boolean variable X120 and so on… with similar behavior task by task.

2.2. Vertical Coordination

This kind of coordination is hierarchic and there are several levels of decision. Each task of a level may control any tasks at a lower level, but never tasks at the same level (Figure 5).

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

The synchronization process is illustrated on a well detailed way in Figure 5 and the SFC of higher level coordinates, at the specific order, 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 and so on...

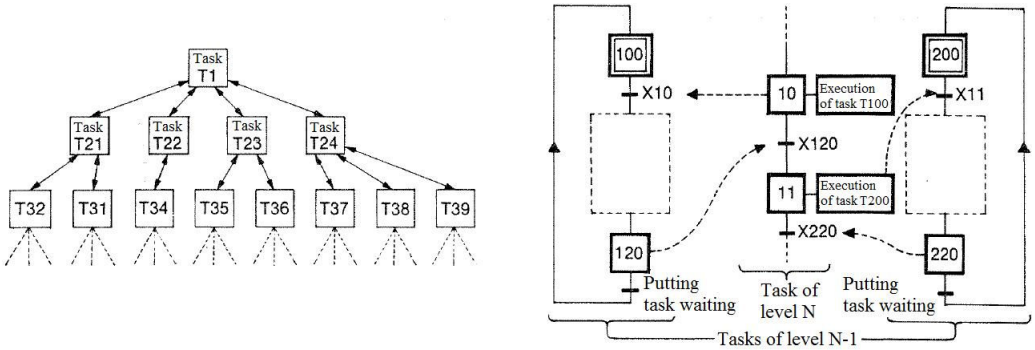

Figure 5. Vertical coordination

This approach is easier to systematize and also is better adapted to treat more complex systems.

3. CASE STUDY

The case study corresponds to an automatic machine of filling and encapsulating bottles (Figure 6). This is divided in three modules, transport and feeding, filling and encapsulating. To increase the productivity, is used a conveyor with several alveoli for the bottles to allow the operation in simultaneous of the three modules.

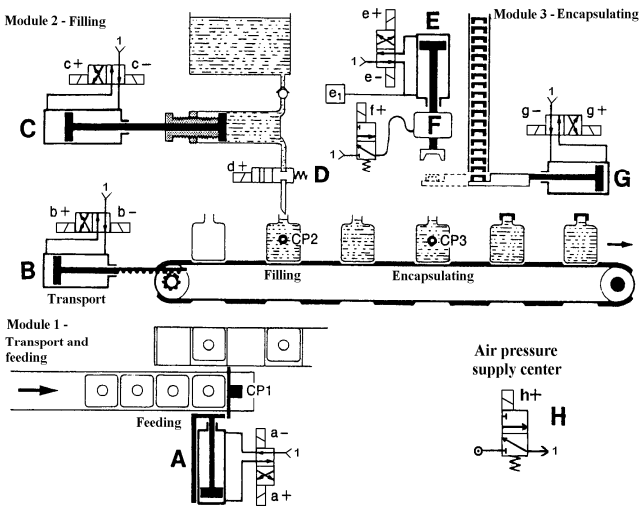

Figure 6. Case study plant.

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

ABCM Symposium Series in Mechatronics - Vol. 4 - pp.408-417

The filling module is composed by a volumetric dispenser, a pneumatic cylinder (C) that actuate the dispenser and an on/off valve (D) to open and close the liquid supply.

The encapsulating module has a pneumatic cylinder (G) to feed the cover, a pneumatic motor (F) to screw the cover and a pneumatic cylinder (E) to advance the cover. The cylinder (E) moves forward until the existent cover, it retreats with this cover during the retreat of (G), continuously it moves forward again with rotation of the motor F to screw the cover.

3.1. Base controller behavior 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, retreated and advanced) and a sensor of pressure e1, which detects the point of contact/stop of the cylinder E in any point of its course.

The valve D and the motor F don't have position sensor because they are difficult to implement.

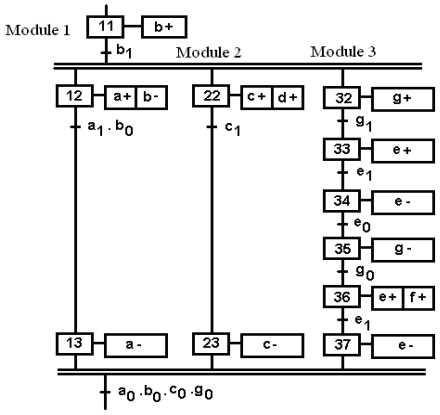

Figure 7. Base SFC controller specification

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, was used the graphic chart of GEMMA because it allows the definition of the run and stop machine tasks.

3.2. Global controller structure

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

A1 – The task A1 "Stop in the initial state" represents the task of the machine represented in the Figure 6.

F1 – Coming of the task A1, when it occurs the start command of the machine, it happens the change for the task F1 "Normal production" (Filling and automatic encapsulating) with the consequent execution of base SFC presented in the Figure 7.

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

F2 – When the machine is "empty" (without bottles) it is necessary to feed bottles progressively, being the machine 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 the task F2 "Preparation mode".

F3 – The "Closing mode" of the 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 encapsulating module is out of service it can be decided to produce in any way, that is, to perform the bottle filling in an automatic way and posterior manual encapsulating, this is main purpose of the task D3 "Production in any way".

D1 – In the case of a situation emergency to occur, the 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), the cleaning and the verification are necessary: this is the purpose of the task A5 "Prepare to run after failure".

A6 – After the procedures of cleaning and verification they be finished 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, to the volume regulation of the bottle liquid dispenser and adjustment of the bottles feeder, a separate command for each movement is required, according to the 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".

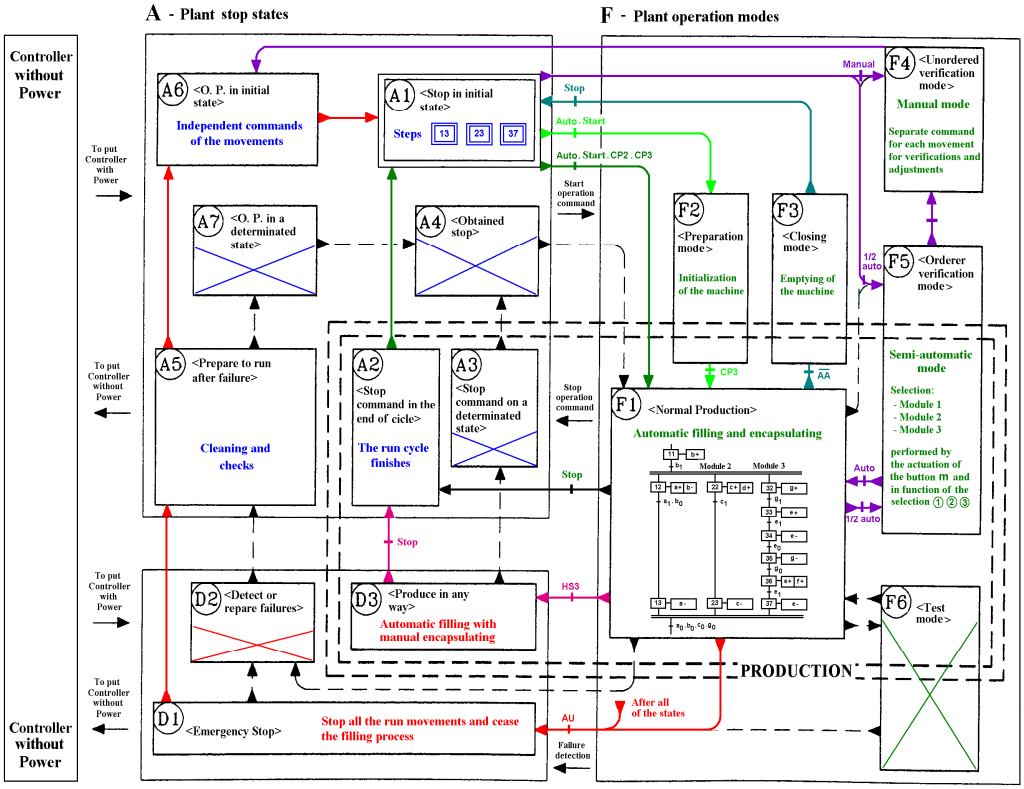

Figure 8. GEMMA of the plant controller.

To be possible the GEMMA evolution becomes necessary existing transition conditions for the run and stop operation modes, 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 (Figure 6);
- Also, it will be necessary a command panel that supplies the transition conditions given by an operator (Figure 9).

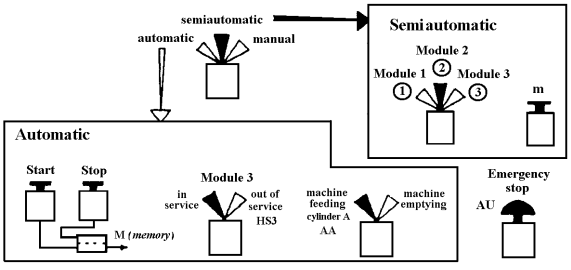

Figure 9. Command panel of the system controller.

In the command panel, there is a main switch that allows selecting the “automatic”, “semiautomatic” and “manual” operations modes.

To the "automatic" option correspond:

- Two buttons "start" and "stop" whose action is memorized in memory M;
- A switch HS3 to put "in service" or "out of service" the module 3;
- 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.

ABCM Symposium Series in Mechatronics - Vol. 4 - pp.408-417

The "semiautomatic" option corresponds to the task F5 "Ordered verification mode", that allows with the actuation of button (m), to check one cycle operation of each modules, selected by the "semiautomatic" switch①,②, or ③.

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

Finally, the AU button (Emergency stop) allows pass to task D1 starting from all of the tasks.

4. COORDINATION OF THE CASE STUDY'S COMPLEX SPECIFICATION

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

- Horizontal Coordination;
- Vertical Coordination.

As showed on section 2, there are several aspects/benefits for each described implementation (vertical coordination and horizontal coordination). However, it seems to be more systematic the vertical coordination because it can be defined two levels of abstraction 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).

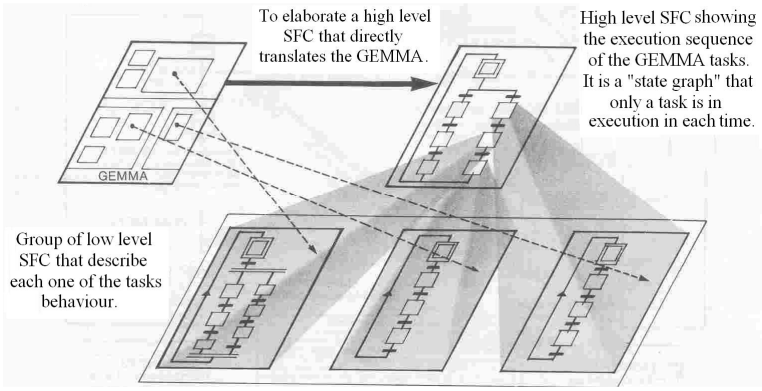

Figure 10. GEMMA implementation with vertical coordination of the multiple SFC

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

1 - Elaborate a high level SFC that directly translates the base GEMMA of the system behaviour;

2 - Elaborate multiple low level SFCs corresponding to each one of the GEMMA tasks;

3 - Synchronization of the SFCs using the vertical coordination method.

4.1. High level SFC

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

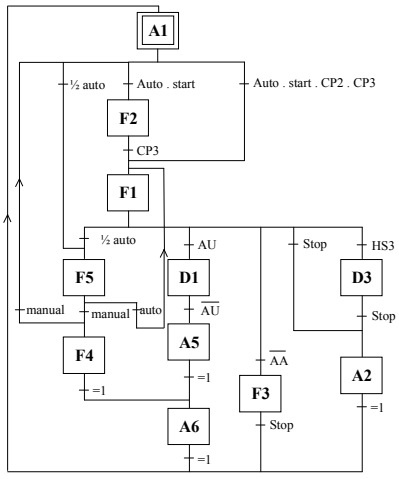

Figure 11. High level SFC.

ABCM Symposium Series in Mechatronics - Vol. 4 - pp.408-417

4.2. Low level SFCs

The development of multiple low level SFCs specifications for each one of the GEMMA tasks considered for the case study plant controller, is the second stage of the vertical coordination implementation of total controller's specification.

In this paper, the SFCs specifications corresponding to the GEMMA main tasks will be shown. This manner, Figure 12 and Figure 13 show the SFC specification, respectively for the tasks F1 "Normal production" and F2 "Preparation mode". The SFC of the task F3 "Closing mode" is not shown because it is very similar to the presented for the task F2. Additionally, Figure 14 and Figure 15 show, respectively for the tasks F5 " Ordered verification mode" and D3 "Production in any way" the SFCs specifications.

It is of highlighted that the "Emergency stop" related with the GEMMA task D1 is not treated, in a detailed way, in this paper, due to its complexity. However, the authors of this paper already presented a publication devoted to this subject (Seabra and Machado, 2009) that presents and discusses a case study with the aim of applies a global approach considering all the automation systems emergency stop requirements. The definition of all the functioning modes and all the stop tasks of the automation system were performed according the respective standards (EN, 1992) (EN, 1997).

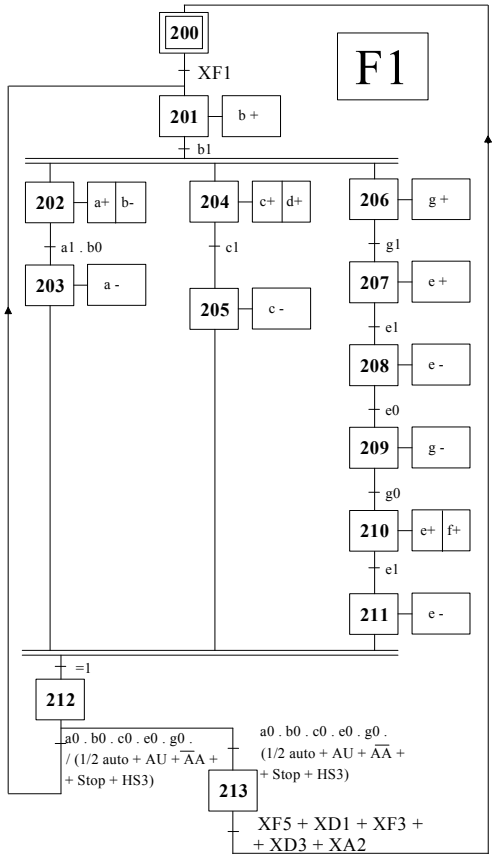

Figure 12. Low level SFC for the normal production task.

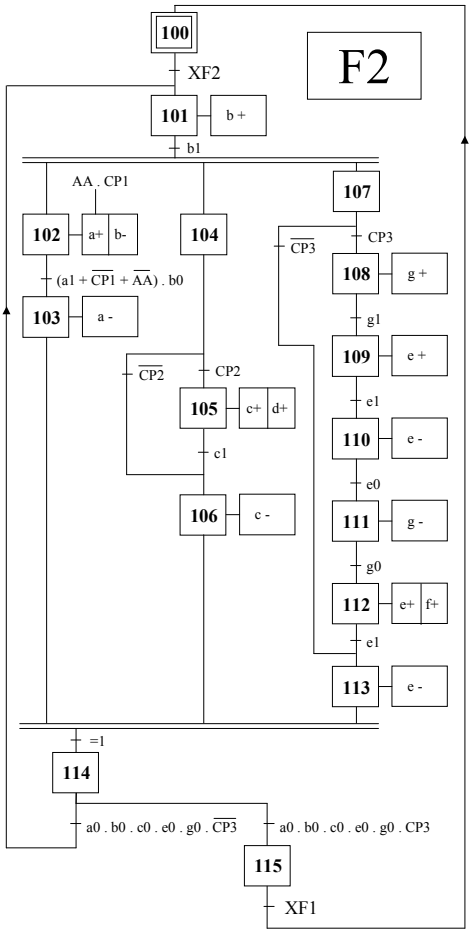

Figure 13. Low level SFC for the preparation task.

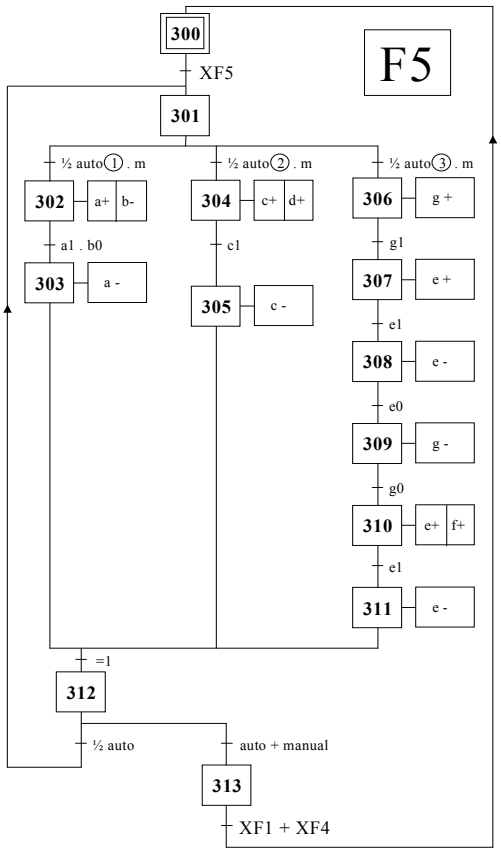

Figure 14.Low level SFC for the ordered verification task.

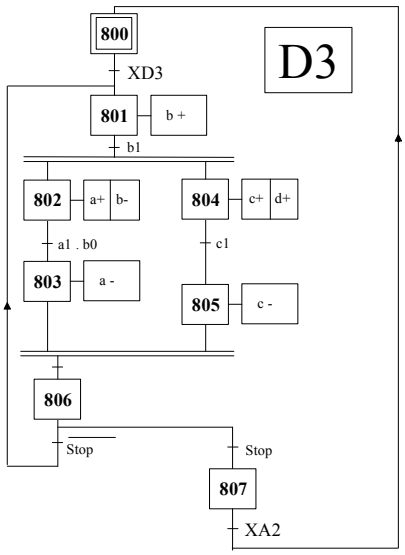

Figure 15.Low level SFC for the production in any way task.

4.3. SFCs synchronization

The last stage of the vertical coordination implementation of total controller's specification it is related with the synchronization of the low level SFCs specifications developed.

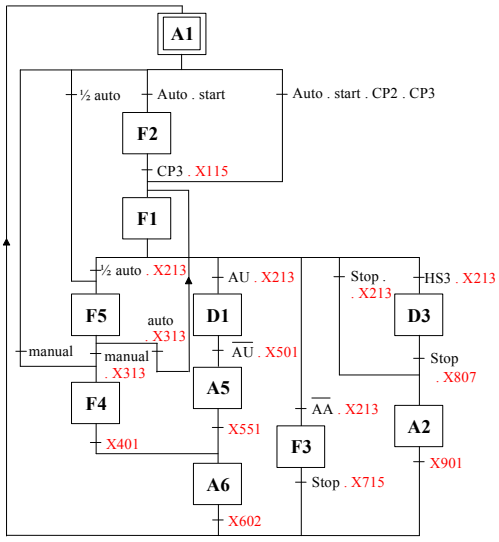

Figure 16. High level SFC completed with low lever SFC step activities (in red).

To achieve this purpose, as described in the section 2, the high level SFC presented in Figure 11 was completed with the SFC step activity/action (Xi - i step number) that correspond to the low level SFC execution stop. Figure 16 shows

the complete high level SFC obtained for vertical coordination implementation (in red they are represented the SFC steps activities added).

All the controller specification, presented on the previous figure, was simulated on Automation Studio Software. The obtained results leaded to the conclusions that all the requirements defined on the Emergency Stop Standards, were accomplished.

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.

All the SFC controller specification, presented on the previous figure, was simulated on Automation Studio Software (FAMIC, 2003). The obtained results leaded to the conclusions that all of the automation system requirements were accomplished.

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 on this publication.

5. CONCLUSIONS AND FUTURE WORK

It was presented,, in a systematic way, the adopted techniques for the deduction of complex specifications for dependable automation systems.

This way, it was explained, first, the use of the GEMMA and the SFC formalisms for the structure and specification of all the system behavior, considering their stop states and functioning modes.

Further, the vertical coordination implementation of a complex total controller's specification, based on the GEMMA graphical chart, was also presented and discussed. This approach may be extrapolated for systems of the same kind.

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

Further work will be devoted, in one hand, to the application of formal methods to verify some important system's behavior properties (taking into account the discrete behavior of the system) and, in other hand, the application of modeling techniques for hybrid systems and respective tools for simulation and formal verification.

6. REFERENCES

ADEPA, 1992. "GEMMA – ADEPA", France.

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

EN, 1992. "EN 418 - Safety of Machinery. Emergency Stop Eequipment, Functional Aspects. Principles for Design". European Standard.

EN, 1997. "EN 60204-1 - Safety of Machinery - Electrical Equipment of Machines - Part 1: General Requirements". European Standard.

FAMIC, 2003. "Automation Studio – User´s Guide", Famic Technologies Inc, Canada.

IEC, 2002. "IEC 60848 - GRAFCET Specification Language for Sequential Function Charts". Edition 2.0 b.

Harel D., 1987, "Statecharts : a visual formalism for complex systems", Science of computer programming North Holland, Vol. 8 pp 231-274.

Koornneef F., and Meulen M.V.D., 2002, "Safety, reliability and security of industrial computer systems" Safety Science Vol. 40, Issue 9, December, pp. 715-717

Moon I., 1994, "Moddeling Programmable Logic Controllers for Logic Verification", IEEE Control Systems Magazine, pp 53-59.

Murata T., 1989, "Petri Nets: Properties, Analysis and Applications", Proceedings of the IEEE, vol. 77, nº 4, April, pp. 541-580

Seabra, E.A.R. and Machado, J., 2009. "Safe Controllers Design for Hybrid Plants: The Emergency Stop", 6th International Conference on Informatics in Control, Automation and Robotics, ICINCO'2009, Milan, Italy; July 2nd-5th.

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

7. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.