6

Supervisory Control of Integrated Building Systems: A Balanced Approach

J.R. Silva[1]
R.L.C.B. Ramos
P.E.Miyagi[2]
University of Sao Paulo, Escola Politecnica
Av.Prof. Mello Moraes, 2231
05508-900 Sao Paulo, SP, Brazil
fax: +55-11-818-5471, e-mail: jorsilva@usp.br

Abstract

This paper presents a formal approach to the design, modeling and simulation of integrated building automation systems. Our main objective is to define a conceptual framework to aid building control system designers in their tasks of specification, analysis, tests and changes of integrated building control strategies. The formal approach proposed can facilitate the development of complete integrated building automation systems, lowering their cost and improving their flexibility, reliability and intelligence (decision making), when compared with the nonformal environments available today. The methodology is based on the supervisory control theory introduced by Ramadge and Wonham, through an input/output interpretation. We claim that a more balanced automation project could be achieved by using this formalism in a net representation called PFS/MFG (Production Flow Schema/Mark Flow Graph), a Petri Net extension. This formalism introduces a hierarchical approach and high level elements to which we attached an estimated time. This formal technique can also represent the interaction between the supervisory system and human operators. The model obtained allows the analysis of behavioral and structural properties of the supervisory control system, including reachability, liveness, invariants and synchronic distances.

Keywords

Petri net, supervisory control, Production Flow Schema (PFS), Mark Flow Graph (MFG), Building Automation Systems, Discrete Event Systems.

---

[1] Partially financed by CNPq.
[2] Partially financed by CNPq and FlexSys Project.

L. M. Camarinha-Matos et al. (eds.), *Balanced Automation Systems II*

1. INTRODUCTION

Microprocessor and computer technology developed in recent years allows a new insight into the benefits an automation system can bring to building owners, tenants and maintenance people. The true integration of heating, ventilation and air conditioning (HVAC), lighting, water supply, security and fire detection systems greatly improves the building safety, comfort, energy conservation, operation and management.

Despite the available technology, very few complete integrated building automation systems have been installed and the 'intelligent building' idea remains a distant reality. Intelligent and truly integrated systems require flexibility (to allow significant changes in the policy of security, lighting, etc without changing the wiring), reliability and also adequate levels of global decision making and interaction between the system and human operators. The environments available today, based on nonformal programming languages and man-machine interfaces with excessive information, cannot satisfy these stringent requirements.

One of the major drawbacks of a poorly integrated building automation system is that the integration and coordination of the various subsystems are left to the operator, which usually is not a person trained for these tasks. This results in frequent occupant comfort complaints, human life and patrimonial safety problems and energy waste.

The key factor in this situation is the design process. Each facility has unique characteristics and the integrated approach makes the requirements specification, tests and simulation difficult tasks, possibly leading to an unreliable automation system. Thus, the development of a formal methodology to design, modeling and analysis of integrated building automation systems is a fundamental step towards more flexible and reliable systems.

The architecture proposed in this paper for modeling of integrated building automation systems is a hierarchical structure of two levels. The local control level is constituted by a set of controllers that execute the basic building control functions, including intrusion controls, fire detection, access control, lighting start/stop and temperature controls. The supervisory control level integrates the various subsystems, providing control patterns, operating modes and setpoints to the underlying level to accomplish the building master plan of safety, comfort and energy conservation.

The local control level is constituted by distributed continuous variable systems (CVS) and discrete event systems (DES), while the decision making supervisor is better represented by a discrete event system (DES), thus originating a hybrid control system.

This hierarchical approach with a supervisor at the top level simplifies the model, allocating standard functions to low level independent controllers and the integrated, more advanced functions, including fault diagnosis, to the supervisory control level. We can say that this structure balances coordination/communication costs and reliability.

Another great advantage of the defined supervisor in realizing the main integration of the building subsystems is that a high level interface to the operator can be created, simplifying the building operation.

In this paper, the system constituted by local controllers/regulators and building utilities/equipments is simply called plant. Thus the hybrid control system can be viewed as a two-level structure with the plant at the bottom level and the supervisor at the top level.

The technique proposed for modeling and analysis of this building hybrid control system is based on the supervisory control theory introduced by Ramadge and Wonham (1989) and on the PFS/MFG net (Silva and Miyagi, 1995, 1996).

2. THE SUPERVISORY CONTROL THEORY

The supervisory control theory provides a suitable formal framework for the control of discrete event systems. The main advantage of this model is that it separates the concept of open loop dynamics (plant) from the feedback control, and thus permits the formulation and solution of a variety of control synthesis problems.

Although the building plant is not constituted by only discrete event systems, a simplified DES plant model can be obtained through a mapping function that transforms continuous state plant variables into a set of discrete events. Since this set of events is chosen by the designer, it is critical to assure that the supervisor receives adequate information to accomplish its task.

The model proposed in supervisory control theory assumes the plant as a discrete dynamic system such that, for each state, a set of events may occur. The plant can be viewed as an event generator and the set of all sequences of events forms a language, modeling mathematically the possible executions of the system.

The supervisor design problem is to modify the open loop behavior of the plant so that the closed loop system meets certain specifications. This requires that the supervisor prevents the undesirable sequences of events from occurring, while enabling the desirable events. Like the discrete event plant, the specification is modeled by a formal language.

Formally, Σ denote the finite set of event labels and Σ^* denote the set of all finite strings of elements of the set Σ, including the empty string ε. A string represents a partial event sample path. The set of all physically possible sample paths is then a subset L of Σ^*. This subset of Σ^* is called a language over the alphabet Σ. A string $u \in \Sigma^*$ is a prefix of a string $v \in \Sigma^*$ if for some $w \in \Sigma^*$, $v = uw$. If v is an admissible sample path, so are all the prefixes of v. If L^* denote the set of prefixes of strings in L, the DES model requires $L^* = L$. In this case, L is called prefix closed. Thus the behavior of a DES is modeled as a prefix closed language L over the event alphabet Σ and each element of L represents a possible event sample path of the DES.

A generator G, which models the plant, is an automaton consisting of a state set Q, initial state $q0$, and transition function δ: $\Sigma \times Q \rightarrow Q$, that is, it is a tuple $G = (Q, \Sigma, \delta, q0)$. The generator G is interpreted as a device that starts in its initial state $q0$ and execute state transitions spontaneously, generating a sequence of events. The transition function δ of G can be extended to a function on $\Sigma^* \times Q$ by defining $\delta(\varepsilon, q) = q$ and $\delta(w\sigma, q) = \delta(\sigma, \delta(w, q))$ if $q' = \delta(w, q)$ and $\delta(\sigma, q')$ are defined. The closed behavior of G is defined to be the prefix closed language $L(G)$, the set of all strings $w \in \Sigma^*$ such that $\delta(w, q0)$ is defined.

To model the control of a DES G, Ramadge and Wonham postulate that certain events of the system can be disabled when desired and that the set of events Σ is divided into uncontrollable and controllable events: $\Sigma = \Sigma u \cup \Sigma c$. The events in Σc can be disabled at any time by synchronization with the supervisor, while those in Σu are the events over which the supervisor has no influence.

A supervisor for G is formally defined as a function $f: \Sigma^* \rightarrow 2\Sigma$, such that $f(w) \supset \Sigma u$, $\forall w \in \Sigma^*$. The set $f(w)$ is the set of events that are allowed by the supervisor to occur, as a function of the string w of past events.

If we denote the closed loop system of G supervised by f by (G, f), the behavior of (G, f), denoted by the language $L(G, f)$, is formally defined as follows:

a) $\varepsilon \in L(G, f)$; and

b) $w\sigma \in L(G, f)$ iff $w \in L(G, f)$, $\sigma \in f(w)$ and $w\sigma \in L \subseteq \Sigma^*$

Now, we can show that the supervisor f can be represented by a DES S, like the plant G. In this case, the control action of S on G is implicit in the transition structure of S. We require that the transitions disabled by f do not appear in the transition structure of S, while the transitions enabled by f and which are possible in G do appear in the transition structure of S. Formally, if $s \in L(G, f)$ then $s \in L(S)$ and $s\sigma \in L(S)$ only if $\sigma \in f(s)$. In addition, if $s \in L(G, f)$, $s\sigma \in L(G)$ and $\sigma \in f(s)$, then $s\sigma \in L(S)$. S and G are assumed to run in parallel such that an event σ can occur when $S \times G$ is in the state (x, q) only if σ is possible in both S and G at that point. The resulting state change is $(x, q) \rightarrow (x', q')$ where $x \rightarrow x'$ and $q \rightarrow q'$ are the transitions in S and G, respectively, under σ. Such a supervisor, realized by a DES S whose behavior is defined by the prefix closed language $L(S)$, can be modeled by a Petri net, allowing property analysis.

Thus, a DES model of a supervisor f is supported by the supervisory control theory, and so is the DES integrated building supervisor proposed in the previous section.

In the original model, the plant is an event generator and the supervisor acts as a passive device, tracking events produced by the plant and restricting its behavior by dynamically disabling the controllable events.

In our approach to supervisory control of integrated building systems, the partition of the alphabet Σ is interpreted according an input/output perspective. The inputs of the plant are constituted by control inputs and disturbances. The control inputs are defined as the set of controllable events (elements of Σc) allowed or forced to occur by the supervisor. The disturbances are defined as the set of uncontrollable events (elements of Σu) that may occur at a given state. The outputs or responses of the plant are modeled by the elements of Σu, driving the state transitions of the supervisor by means of observed plant state.

The generation of events is therefore initiated not only by the plant, but also by the supervisor (Balemi, 1993, Garcia, 1994). This supervisor model can accomodate high level operator commands through a suitable man-machine interface.

Thus, the resulting closed loop control system is composed by a discrete event model of the building plant controlled by a discrete event supervisor capable of action enforcement. The DES supervisor and the simplified DES plant allow the integrated building hybrid control system to be modeled as two interacting discrete event systems, which are more easily analyzed than the system in its original form.

3. THE FORMAL REPRESENTATION OF THE BUILDING SUPERVISOR

An integrated building plant consists of a large number of subsystems which operate in parallel resulting a huge state space. The synthesis procedure covered by the supervisory control theory generates an abstract supervisor specification which is not directly usable for practical implementation. Moreover, designers have to face a dicotomy: it is very difficult to achieve a good integration and modularization among subprocesses (such as heating, lighting, security, etc) without a formal model and representation, and, in the other hand, it is hard to impose a sound mathematical framework that also covers the need for flexibility, expressibility and synchronization of processes.

The synchronization of processes and actions are important to the modeling of integrated building supervisor and plant processes. In addition, behavioral and structural property analysis of the building supervisory control system is crucial to assure its reliability. To address these

problems, a Petri net (Murata, 1989, Peterson, 1981) representation of the DES supervisor is proposed . The need of a more synthetic model and a more structured design methodology implies the choice of a high level extended net.

A hierarchical approach called PFS/MFG (Silva and Miyagi, 1995, 1996), based on Condition/Event Petri nets, fits the requirements of integrated building supervisory control systems through high level static and dynamic elements.

Each static element called box can represent a single element or a 'static composed element', that is, a subnet. The PFS/MFG approach also includes abstract elements called activities. Activities stand for an entire subnet and introduce the concept of 'dynamic composed element'.

In a large model like the integrated building automation system, activities are essencial in encapsulating behavior of processes and subsystems. A partial model can be obtained and simulated regarding only the main elements of the system and the interactions between them. To refine the partial model, a pointer to another subnet should be added to the original object representation and internal elements would connect and synchronize the aggregated subnet. In PFS/MFG there is also the sub-class time-box, which has a parameter with the estimated time to enable the firing.

Another special PFS/MFG element is the gate, which consist of a kind of flux or relation between static and dynamic elements originated by external conditions. Gates can be useful to represent human operator commands to the integrated building supervisor, such as manual/automatic switches.

The formulation of a new state equation to describe a system behavior, based on the duality of PFS/MFG, permits an analytical treatment of the behavioral and structural property analysis of the building supervisory control system, including reachability, liveness, invariants and synchronic distances.

We use PFS/MFG as a more expressible net representation which is a morphism to a prefix closed language and consequently to a supervisory specification. Abstract elements (activities) are used to express a process whose internal behavior is not in concern when we analyse its interaction with other processes (separation of concerns). Similar abstraction can be obtained from static elements (boxes) which can store message queues, for instance. Finally the introduction of gates and permanent markings are used to provide connection (dependencies) among related processes and pseudoconditions (or pseudoboxes) can stand for signals exchanged between the system and the outside, including actions launched by human operators.

A balanced automation is crucial in this domain, since modular automation tasks and subsystems have to be integrated by a combination of automated processes and human intervention, in order to achieve a good level of automation reliable and secure. Thus, formal model and partial representation of the interaction between the system and operator signs have to be combined in the same framework.

4. EXAMPLE OF AN INTEGRATED BUILDING CONTROL APPLICATION

In this section, a simple illustrative example is given to clarify the above concepts. Here we consider a building plant subjected to security and comfort constraints. If a person enters a room, an operator must be advised by a visual alarm, through a lamp relay command. The room temperature must be maintained in a narrow comfort band to assure occupant comfort. To conserve energy, the room setpoint temperature must be raised if the room is unoccupied.

To simplify our analysis we consider that the room temperature can be switched between two setpoints, *setp0* and *setp1*, with *setp0* < *setp1*.

To design a suitable integrated building automation system to this application, we have initially to choose the best architecture to the model. The structure proposed in this paper is organized into two levels, in order to balance the coordination costs and the reliability. According to this schema, the local control level for this application must be constituted by independent room DES security controllers and CVS temperature controllers, to execute the basic control functions, that is, the intrusion detection/alarm and temperature regulation. The energy conservation and fault diagnosis functions are left to the high level supervisor.

The next step in the modeling process is to obtain a simplified DES model for the DES/CVS plant. We can do this by defining various discretized room temperatures. The whole temperature range can be partitioned into small ranges, with the limit crossing of each range associated to an event.

The use of standard controllers at the local control level simplifies the plant model and analysis. The design complexity is in the supervisor model, which realizes the specific integrated advanced functions.

We can represent the plant in this example by two automata models for the security and thermal comfort subsystems. For simplification purposes, we consider the control system attending only one room. The event alphabets of the subsystems are:

Σsec = {*r_occupied, r_unoccupied, c_alarm*}

Σtco = {*c_setp0, c_setp1, temp_0, temp_1, c_open_valve, c_close_valve*}

where, *temp_0* and *temp_1* are the events associated to the temperature ranges and *c_open_valve* and *c_close_valve* are the commands to the chilled water valve of the room air handling unit.

The complete set of event labels of the plant is $\Sigma = \Sigma sec \cup \Sigma tco$. According to the supervisory control theory, this set Σ can be divided into two subsets: Σu, the set of uncontrollable events and Σc, the set of controllable events over which the supervisor has authority. Thus we have:

Σu = {*r_occupied, r_unoccupied, c_alarm, temp_0, temp_1, c_open_valve, c_close_valve*}

Σc = {*c_setp0, c_setp1*}

The specification for the building automation system is that the room temperature must be regulated to the low setpoint *setp0* if the room is occupied and to the high setpoint *setp1* if the room is unoccupied, in order to conserve energy. A supervisor S for the plant must be designed such that the closed loop system meets this specification.

This requires that the supervisor S allows the event *c_setp0* to occur only if the room is occupied and in this case the event *c_setp1* is disabled. Moreover, if the supervisor receives the event *r_unoccupied* from the plant, the event *c_setp1* is enabled and *c_setp0* is disabled.

We showed previously that this supervisor S can be represented by a DES model, where the control action of the supervisor on the plant is implicit in the transition structure of S. In this example, the synthesis of the supervisor can be done manually, but in a more general case it is easy to see that the manual design without high level tools may be a cumbersome and unreliable task.

The Figure 1 shows a PFS/MFG model of the supervisor for the temperature system.

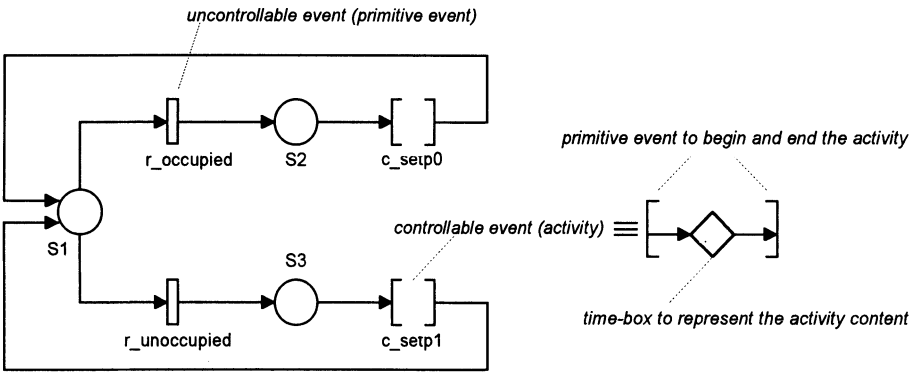

Figure 1 PFS/MFG of the temperature supervisor system.

The PFS/MFG model allows the temperature control process to be encapsulated by a dynamic element activity, representing the interaction between supervisor and plant processes in a easier form.

The above example illustrated the design method proposed for integrated building automation systems. It is important to note that the main advantages of our formal hierarchical approach are the flexibility and reliability of the final control system. With this scheme, building changes can be more easily accommodate, reducing engineering costs.

5. CONCLUSION

We presented a formal approach to design and modeling of integrated building automation systems. The method proposed is based on the supervisory control theory and on the PFS/MFG extended Petri net. The DES supervisor interacts with the simplified DES building plant to accomplish the building specifications of safety, comfort and energy conservation. This formal methodology allows property analysis and simulation, improving the system reliability.

We believe that the formal approach proposed in this paper is the right answer to the stringent requirements of integrated building automation systems, which include flexibility to accomodate frequent building operational and structural changes, reliability, decision making and a high level interface with useful and preprocessed information to human operators.

The software tools available today from several building automation system manufacturers still don't allow the adequate balance between the control system and the operators. The nonformal programming languages, the powerful graphical tools to create supervision screens, the preprogrammed 'canned' routines and the application specific controllers induce the designer to specify systems with low level of integration and intelligence, normally executing only basic building control functions. In this scenery, the operators monitor the building systems through several screens, windows and icons plentiful of information that they can't process during day-to-day operations. In general, these systems only 'mimic' the older security and fire central systems, analog temperature controllers and lighting timers, not realizing the

great benefits of integrated control and decision functions made possible by the current microprocessor technology. These factors limit the benefits of integration to a few large building control projects. The formal techniques described in this paper can extend intelligence and integrated functions to a large number of buildings of several sizes, allowing the designers to specify the desirable and unique characteristics of each project.

Some work using this formalism to model subsystems such as elevators (Miyagi et al., 1995) has been developed. Future research efforts include theoretical aspects of the supervisory system, the evaluation of artificial intelligence techniques to model the decision making process and the implementation of an environment for modeling, synthesis, analysis, simulation and generation of integrated building supervisory control systems.

6. REFERENCES

Balemi, S. et al. (1993) Supervisory control of a rapid thermal multiprocessor. *IEEE Transactions on Automatic Control*, vol.38, no.7, pp.1040-1059.

Garcia, H.E., Ray, A. and Edwards, R.M. (1994) A reconfigurable hybrid supervisory system for process control. *Proceedings of the 33rd Conference on Decision and Control*, Lake Buena Vista, FL, pp.3131-3136.

Miyagi, P.E, et al. (1995) Training system for control design of discrete event systems, *Preprints of 4th IFAC Symposium on Low Cost Automation*, Buenos Aires.

Murata, T. (1989) Petri nets: properties, analysis and applications. *Proceedings of the IEEE*, vol.77, no.4.

Peterson, J.L. (1981) *Petri net theory and the modeling of systems*, Prentice-Hall, Englewood Cliffs, NJ.

Ramadge, P.J. and Wonham, W.M. (1989) The control of discrete event systems. *Proceedings of the IEEE*, vol.77, no.1.

Silva, J.R. and Miyagi, P.E. (1995) PFS/MFG: a high level net to the modeling of discrete manufacturing systems, In: Camarinha-Matos, L.M. and Afsarmanesh, H. (Eds.) *Balanced Automation Systems - Architectures and Design Methods*, IFIP/Chapman & Hall, London.

Silva, J.R. and Miyagi, P.E. (1996) *A formal approach to PFS/MFG: a Petri net representation of discrete manufacturing systems* to appear in *Studies in Informatics and Control*, IC Publications, Romania.

Stiver, J.A. and Antsaklis, P.J. (1992) Modeling and analysis of hybrid control systems. *Proceedings of the 31st Conference on Decision and Control*, Tucson, Arizona.

7. BIOGRAPHY

Dr. José R.Silva is Assistant Professor of the University of Sao Paulo, Brazil. His research interests are in design theory, software engineering, intelligent CAD.

Roberto L.C.B.Ramos is in the postgraduate program of University of Sao Paulo, Brazil. His research interests are in discrete event systems, software engineering, intelligent buildings.

Dr. Paulo E.Miyagi is Associate Professor of the University of Sao Paulo, Brazil. His research interests are in discrete event dynamic systems, design of control systems.