Bulletin de la Société Royale des Sciences de Liège, Vol. 85, 2016, *p*. 756 - 765

Using of supervisory control theory in emergency shout down control system of an off-shore gas platform

Seyede Fatemeh ASHRAFIAN[1,*], Abbas DIDEBAN[2]
[1] Ms student of electronic eng.
[2] Associate Professor, Semnan University, Semnan, Iran

Abstract

This paper focuses on modeling of emergency shut-down control system in an off-shore gas platform using petri net. Considering the nature of the safety control system in industries, it can be considered as a discrete event system. In this regard, first the equipments under emergency shutdown system along with the rules that govern how they act are modeled. Then, the local shut down in all unit separately , after that, process shut down which rules the performance of process unit equipment in emergency situation, in the next step, high level emergency shutdown (level 1) and the platform emergency shut down as a hierarchical modeling system are modeled . Finally by combining the models, the final structure implementable on programmable logical controller was modeled by Snoopy software. The full model contains details of all units and criteria governing them, we suffice to mention excerpts of the entire designed model.

Key words: Petri Net, discrete Event System, supervisory control, emergency shutdown system, offshore platform safety instrument system.

1. Introduction

With the advancement of industries and the rapid growth of technology in different fields, particularly in high-risk industries, the issue of safety control systems as a vital part of the work is of extraordinary importance, and hence has been investigated with different viewpoints. It has also been considered by engineers, manufacturing companies, researchers and scientific forums who have an applied and industry-oriented view. The topic to be discussed in this article is the modeling of emergency shut-down system as an essential component of the safety control system in an off-shore gas platform.

Because of the importance of safety control systems studies have been so far done on this subject, the main pillar of which in the issue of principles and methods of hazard identification and detection, estimation and risk assessment [1, 2, 3]. A significant part is the characteristics and requirements of the equipment and hardware used in the systems [4]. Other part is devoted to subject of the logic of the software used in the safety control system as the

* Email address : f16ashrafian@yahoo.com

mastermind of the system. For example we can imply to some research and scientific activities in this field include [5, 6, 7, 8, 9].

Considering the nature of the safety control system in industries, it can be considered as a discrete event system. A variety of tools can be applied for the analysis of discrete event systems that can generally be divided into three groups: graphical, algebraic and systematic language-based tools, each having its own application. The first group consists of the Automata, Flow diagrams, Ladder diagrams, Grafcet and Petri nets [10]. As can be seen, automata and state diagram are used under the activities mentioned above. At the same time, it can be seen that on one hand the related modeling is generally focused on relatively smaller limits due to the limitation of these methods, and on the other hand, mainly, the verification of the function of safety system in separated limits has been verified. In relatively complex systems, the automata system is affected by an explosion of states, and hence, it cannot be used in modeling of huge systems. Ladder diagrams are very bulky and inefficient for complex systems. Grafcet can be considered as a subset of Petri net [11]; However, todays the use of Petri nets is broader and more inclusive. Petri net is a mathematics-based method making mathematical concepts and relations understandable and analyzable using a graphical tool. This method has been considered and welcomed in modeling and analysis of different systems such as industrial and robotic automation [12] and chemical block activities [13] analysis of the behavior of shut down safety system in the nuclear industry [14] and other items.

Given the importance of safety in the Hydrocarbons industry and in particular oil and gas offshore platforms, petri net based modeling of emergency shutdown system in a fixed offshore sour gas production platform is studied this paper .In this regard, the equipment under emergency shutdown system along with the rules that govern how they act in emergency situation are modeled. . In the following stages the process shut down level (ESD2), which rules the performance of process unit equipment in emergency situation is modeled. At higher levels, emergency shutdown (ESD1) which in addition to the disconnection effects, turns the utility units to emergency shutdown mode is modeled. At the top level the platform emergency shut down (ESD0) as a hierarchical modeling system is modeled. Finally by combining the models, the final structure implementable on programmable logical controller was modeled by Snoopy software. Through exploring different scenarios of events happened and also a variety of scenarios of risks that may arise, it could achieve acceptable results**.**

2. Petri Net

Petri net is a tool based on mathematics with a graphical expression that has found a wide application in modeling and analysis of discrete event systems [15].Using Petri net, in addition to the fact that the visualization of processes can prevent some programming errors or the problem of staying out of sight in some circumstances in designing, in comparison with algebraic methods. Because the states are put next to each other, instead of multiplying them

like a state diagram, state explosion[†] and bulking the model and the problem of making it impossible to control the visual model are also prevented. Petri net tools include the following items: place (indicating different system state), transition (indicating events or factors changing the state of the system), arc (indicating the system changes following the occurrence of events) and token (presence of one or more solid circles indicates the activeness of the mode of that place). Figure 1.

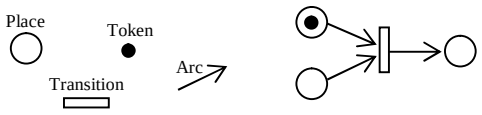

Figure 1: Petri net elements

Supervisory control theory provides a systematic method to model the control system that is a method for automatically synthesizing supervisors that restrict the behavior of a plant so that as much as possible of the given specifications are fulfilled [16].

3. Safety Instrument System (SIS)

A control system designed and applied to perform one or more safety control measures. A safety instrumented system (SIS) is composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when predetermined conditions are violated. The system may also be called as different names since it has been implemented in different forms. The very important advantage is the independence of this system from basic process control system [17, 18].

Shutdown systems provide an instrumented means of protecting plant and equipment from conditions outside the design basis. By isolating inventories and effecting blow down they also provide means for mitigating some of the hazards arising following loss of containment.

4. Platform Production Process

The fixed gas production offshore platform is being studied, and consists of several process and utility units. Briefly, and aside from details, it can be said the process operations done on the platform includes the separation of water and condensates from the gas (to prevent and reduce corrosion of transmission pipelines and associated equipment). Well fluid enters Free Water Knockout Drum (FWKO) then the condensate coalescer through production manifold and loses its water and moisture through these two stages. Finally the gas and condensate which have lost their water and moisture to some acceptable extent are mixed and transferred

[†] The exponential increase of the number of global states, and hence the complexity of the analysis, with the number of components.

to onshore refineries via marine pipelines for processing and export. The water separated from these two stages is routed to the water treatment unit. The test separator unit also features a benchmark for testing the features of exhaust gas of any wells before entering that into the production process. Flare system and multiple other utilities are located on the platform to meet the needs of the process. [19]

5. Modeling of Platform Emergency shutdown Control System

In the safety control system we discuss, depending on the type and extent of the errors, deviations and consequences of their occurrence, emergency shut-down is considered in hierarchical manner. It comprises the highest level as abandon platform shut-down, then emergency shut-down, after that process shutdown and finally the lowest level as local shutdown. Any unit is considered as a subsystem, which is in its turn divided to its components. The rule governing each unit is determined by local shut down commands and rule governing more than one unit is determined by emergency shut-down status of the higher levels. The inputs of the system include alarms which can be activated by corresponding first elements (such as sensors or switches), alarm signals receive from the systems associated with it (such as process control system or fire & gas system) and dedicated push buttons. The controllable components of each unit are composed by final elements including actuators of the emergency shut-down valves, blow-down valves and pumps.

In this paper, due to the high volume of the entire models and final completed model, it is impossible to explain all modeled parts. There for we suffice to Petri net model of one type equipment of the system and the rules governing them(back to back pumps), Petri net model of “two of the three voting logic” used in special cases (as a rule), top model of Hierarchy including emergency shut-down, ASD, ESD and PSD levels along with the Petri net model of system start up, and bringing Petri net model discrete units that make up the sub system is avoided.

5.1. Petri net Model of Back to Back Pumps

In some units we use of 2 back to back pumps. At any time one pump is working and the other is in standby mode. In case of failure in the operation of the working pump, the other pump is automatically turned on. In the example selected, the pumps are related to unit 42 (chemical injection). Petri model is distinguished as gray color for the first pump, black color for the second, and lavender color for the Petri model of the rule governing them. In the case of local shut-down in that unit, the command to shut down the pump is issued by sending one token from unit’s local shutdown rule or from higher level shut down to place ”p4201” that turns the running pump into stop mode. The Petri net model of Back to back pumps is illustrated in Figure 2 along with the rules governing their operation.

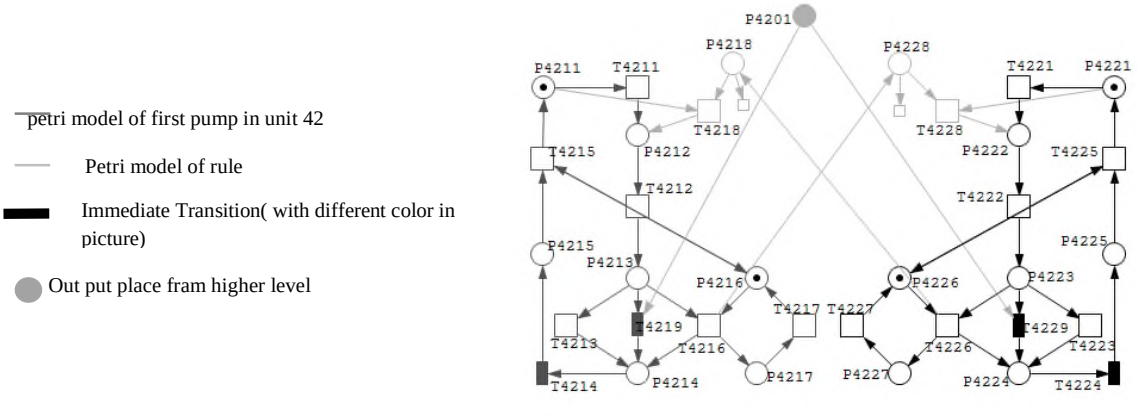

Figure 2: Petri nets model of back to back pumps

Table 1: Description of pumps petri model place and transition

Place / transition	Description	Place / transition	Description	Place / transition	Description
P4211/P4221	Pump 1/2 Ready	T4213/T4223	Pump 1/2 to Stop Manualy	P4216/P4226	Pump 1/2 Correct
T4211/T4221	Pump 1/2 to Start	P4214/P4224	Pump 1/2 Stoping	T4216/T4226	Pump 1/2 fauiler
P4212/P4222	Pump 1/2 Starting	T4214/T4224	Pump 1/2 status signal OFF	P4217/P4227	Pump 1/2Un correct
T4212/T4222	Pump 1/2 status signal ON	P4215/P4225	Pump 1/2 OFF	T4217/T4227	Pump 1/2 Repaired
P4213/P4223	Pump 1/2 ON	T4215/T4225	Pump 1/2 Reset	P4201	Shut down from top level

5.2. Voting's petri net model

In some cases where there is the need to further insurances of real situation before the system reaction, and action of safety control system to detect deviations of the measured parameter, which entails emergency shutdown at high levels, the M out of N voting logic is applied briefly called MOON. In this case, the system intervenes only if at least M of N related sensors show the specific parameter deviation. For example, on our offshore gas production platform, the Export line which transfers the platform products into onshore refinery is equipped with three pressure transmitters. These three transmitters can produce very low pressure alarm (PALL) that may indicate rupture or breaking of pipeline or very high pressure (PAHH) that indicates the line blockage. This alarm initiates system emergency shutdown level. In this example, if two of the three sensors used produce alarm, the system will take the appropriate action. If a transmitter fails, the system deems the information given by that as invalid and will continue to operate with the two remaining transmitters with 2oo2 voting logic until it is completely fixed or replaced with an correct and integrated transmitter. The petri net model of this logic, illustrated in Figure 3.

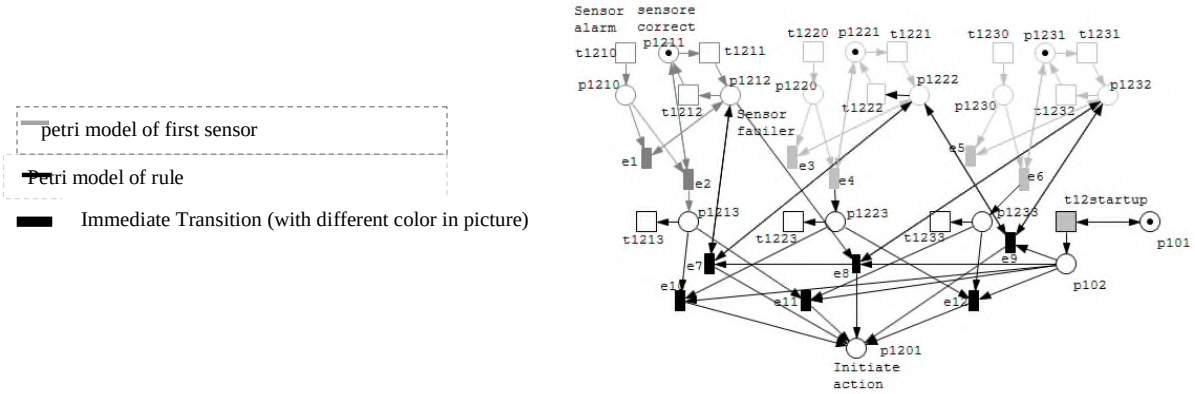

Figure 3: Petri model of voting 2 of 3

Table 2: Description of voting 2 of 3 Petri net model place and transition

Place / transition	Description	Place / transition	Description
T1210/T1220/T1230	Sensor 1/2/3 produces alarm	P1211/P1221/P1231	Sensor 1/2/3 UnCorrect
P1211/P1221/P1231	Sensor 1/2/3 Correct	T1212/T1222/T1232	Sensor 1/2/3 Repaired
T1211/T1221/T1231	Sensor 1/2/3 Failed	P1201	Initiate proper action

5.3. Petri net model of emergency shutdown system hierarchy

The ESD system will be configured with a hierarchy of levels that are progressive in their effects. ESD 0 total shut down ('Black Shutdown') and abandon platform, ESD 1 emergency shutdown and depressurization, ESD2 process shutdown and ESD 3 equipment or package shutdown. Each level of shutdown may be activated by the operator and in some instances automatic initiation occurs. Higher levels automatically initiate lower levels.

ESD 0 is intended for use in situations that pose major hazards to the integrity of the entire platform. Examples would be large fires, major loss of containment of flammable gas or liquid, or earthquakes affecting the area. ESD 0 brings about a total black shutdown of the platform. All process and utility systems are shut down and potential sources of hazard and ignition are isolated, ESD 1 is initiated and blow down of the process systems occurs. This level of ESD is manually initiated from its pushbuttons at key locations on the platform (such as helideck and boat landing) and may also be initiated from a pushbutton in the central control room.

ESD 1 is a response to the confirmed detection of fire or gas leakage on the platform or to other hazards of a serious nature that threaten major areas of the platform. This level of ESD is initiated either manually or automatically. Manual initiation is considered as Pushbuttons in the key point locations on the platform and central control room, and Automatic initiation occurs as ESD 0 or special hazardous situation, for example Fire or Gas detection, Wellhead control system failure, ESDV hydraulic fluid failure. In addition to those occurring at the lower ESD Levels, shut down of all utility units occurs too at this level of

ESD. It results in the shutdown of all process and utility systems on the platform and automatic blow down.

ESD 2 (process shut down) applies to deviations of process or utility system conditions outside allowable limits that have potentially serious implications for platform safety. Process shut down is initiated either manually or automatically. Manual initiation is considered as pushbuttons in special points on the platform and in the central control room. Automatic initiation occurs as ESD 1, Total loss of power generation, Production manifold high pressure, platform export line high/low pressure and other excessive deviation of operating conditions in major process or utility systems. Closure of all ESDVs resulting in isolation of all process and utility systems (power generation remains available), Stop chemical injection and initiating of some ESD Level 3 occur at ESD 2. In other hand all process units are shut down in this level.

ESD 3 brings about the shutdown and isolation of individual equipment items or packages. It may be initiated by activation of manual software shutdown buttons for individual equipment items, automatically by deviations of significant process or equipment conditions resulting in specific equipment isolation or shutdown or by the initiation of higher shutdown levels. The typical actions resulting from ESD 3 are the stopping of rotating equipment, the removal of heat sources (where applicable), the closure of isolation valves.

Top model of Hierarchy including emergency shut-down, ASD, ESD and PSD levels along with the Petri net model of system start-up are presented in figure 4, and bringing Petri net models of discrete units that make up the sub system is avoided.

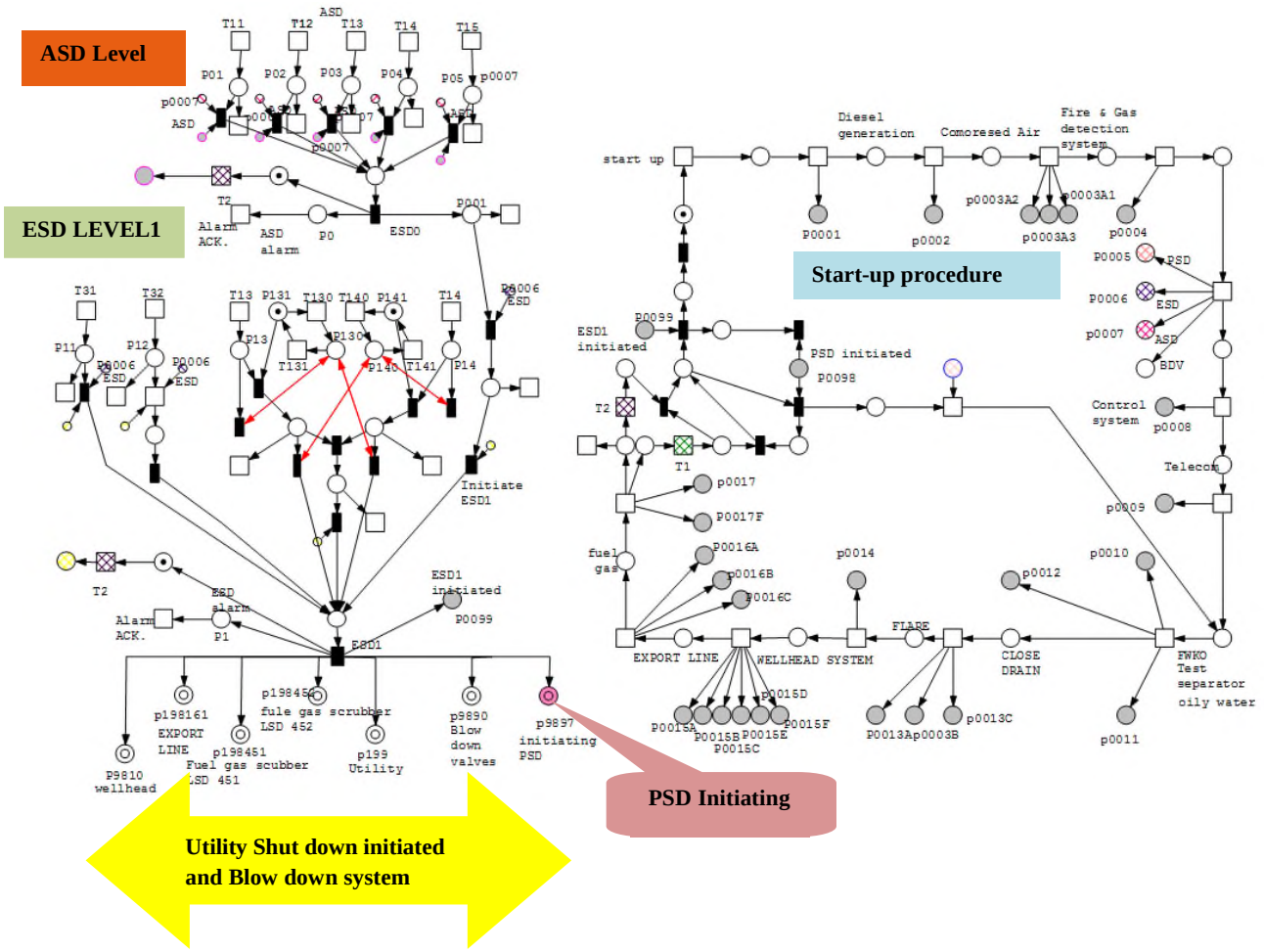

Figure 4: Petri model of emergency shutdown system hierarchy with start-up procedure

6. Verification

Snoopy software was used to ensure the integrity of the model performance. Possible deadlocks and not proper response to any possible situation were examined using this software, and various scenarios were tested with the results obtained being satisfactory. With each alarm the model receives from stimulus points at different levels as the parameter's crossing their limit, the model shows appropriate response as a logic solver. It should be noted that snoopy software used in this modeling, in addition to the ability it has in designing hierarchical and simulation systems and related charts, it also has the capability to convert and transfer the designed model to a model to be used in Matlab. More studies may be more advantageous in this regard'.

7. Conclusion

Given the nature of the emergency shutdown control system, describing and defining it as a discrete event system makes it easier to understand system performance and, ultimately, its control system design and also minimizes human error in the controller designing stages. Different methods have been used to describe the performance of these systems, in most of which automata and state diagram are used (almost for small and limited cases). A major weakness of the state diagram and automata is the problem of state explosion in modeling relative large systems that reduces its performance and make it difficult to tracing and analyzing the behavior of model. On the other hand, modeling with this tool has been mainly used regarding the verification of safety systems in particular areas. Use of Petri net tools in modeling, in addition to having a strong background in mathematics has a certain attraction due to the illustrations in the control process. By the way, because the system states are located beside each other and to avoid the multiplication of states, the resulting model would be less compact and it would be more possible to examine its performance, trace its behaviors and predict different scenarios. Given the systematic nature of designing method and use of supervisory control theory, probability of error in prediction of possible deviations is reduced, the ignorance of which in designing the system can be disastrous in the future. In the supervisory control theory, two models of systems and rules should be formed and the final control should be obtained by combining them. At these stages, the combination of methods at the classified levels has been used to facilitate the modeling. This method can be used both to display dynamic performance of the system and reduce potential human errors in designing the controller. The full model contains details of all units and criteria governing them, in this article we suffice to mention excerpts of the entire designed model. The final obtained model can be well implemented on programmable logical controller (PLC) and has practical application.

References

[1] Roy E. Sanders. (2005), “Chemical Process Safety”, Elsevier butter worth–Heinemann, ISBN: 0-7506-7749-X.
[2] In Jae Shin, (2014), “Loss prevention at the startup stage in process safety management: From distributed cognition perspective with an accident case study”, Loss prevention in the industries, 27, pp.99-113.
[3] Feng Wang, Yankun Zhao, Ou yang, Jingbo Cai, Mei Deng (2013),“Process safety data management program based on HAZOP analysis and its application to an ethylene oxide/ethylene glycol plant” ,Loss prevention in the industries , 26,pp.1399-1406.
[4] German Luna-Mejias, (2013) “Using ESD Valves as Safeguards, Myth or Reality”, 9th Global Congress on Process Safety San Antonio, Texas.
[5] Jinkyung Kim, Younghee Lee, Il Moon. (2007),” Modeling and Verification of Control Logics in Safety Instrumented System for Chemical Industrial Processes”, 17th European Symposium on Computer Aided Process Engineering – ESCAPE17 V. Plesu and P.S. Agachi (Editors).

[6] Junbeom Yoo, Eunkyoung Jee, Sungdeok Cha. (2009), “Formal Modeling and Verification of Safety-Critical Software” IEEE computer society, IEEE software.
[7] Dallas L.Green, Arthur M.Dowell, III, P.E. (1995) “How to design, verify and validate emergency shutdown systems” ISA transactions 34. Pp.261-272.
[8] Valkonen, Janne; Björkman, Kim, Frits, Juho; Niemelä, Ilkka, (2010),” Model checking methodology for verification of safety logics” SIAS 2010 - The 6th International Conference on Safety of Industrial Automated Systems.
[9] S. Manesis, K. Akantziotis, (2005), “Automated synthesis of Ladder automation circuitsbased on state-diagrams”, University of Patras, Electrical and Computer Engineering Department, Elsevier Ltd, Advances in Engineering Software 36, pp. 225–233.
[10] B. Hruz, M.C. Zhou (2007),” Advanced text books in control and signal processing: modeling and control of discrete-event dynamic systems”, Springer-Verlag London Limited.
[11] Zulhairi bin othaman, (2005),”Comparision of rll, state diagram, grafcet alId petri net for the realization of logic controller” kolej university teknologi TUN Hussein NN.
[12] M.F. Russo, (2008)"Modeling, analysis, simulation, and control of laboratory automation systems using Petri nets analysis and control," The association for Laboratory automation, vol.13, pp.103-115.
[13] D. Andreu, J.C. Pascal, H. Pingaud, R. Valette,(1994), "Batch process modeling using Petri nets," IEEE International conference on systems, man and cybernetics, pp.14-319.
[14] Seung MO Cho, Hyoung Seok Hong, Sung Deok Cha, (1996), “Safety Analysis Using Coloured Petri Nets” Korea Advanced Institute of Science and Technology (KAIST) Department of Computer Science
[15] B. Hrúz and M.C. Zhou, (2007),”Modeling and Control of Discrete-event Dynamic Systems”, Springer-Verlag London Limited.
[16] Ramadge P. J., Wonham W. M. (1987), “Supervisory control of a class of discrete event processes”. Journal of Control and Optimization, Vol.25, No1.
[17] Mary Ann Lundteigen, (2009), “Safety instrumented systems in the oil and gas industry”, Norwegian University of Science and Technology.
[18] Jennifer L. Bergstrom, (2009), “Safety Instrumented System (SIS) and Safety Life Cycle”, *Process Engineering Associates, LLC*, http://www.Processengr.com.
[19] Havard Devold, (2013),”Oil and gas production handbook”, Edition 3, ABB company, ISBN 978-82-997886-3-2.